Intelligence Transformation: Using Threat Characteristics to Define Division Capabilities

A Monograph

by

Major Frank A. Smith

United States Army

School of Advanced Military Studies

United States Army Command and General Staff College

Fort Leavenworth, Kansas

AY 05-06

REPORT DOCUMENTATION PAGE

Form Approved
OMS No. 0704-0188

1. REPORT DATE *(DD-MM- YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
25-05-2006	**MONOGRAPH**	**SEPT 2005-MAR 2006**

4. TITLE AND SUBTITLE
INTELLIGENCE TRANSFORMATION: USING THREAT CHARACTERISTICS TO DEFINE DIVISION CAPABILITIES

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ Frank A. Smith

5d. PROJECT NUMBER

***5e.* TASK NUMBER**

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies
250 Gibbon Ave
Ft. Leavenworth, KS 66027

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Command and General Staff College
1 Reynolds Ave
Ft. Leavenworth, KS 66027

10. SPONSOR/MONITOR'S ACRONYM(S)
CGSC, SAMS

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This monograph explores the intelligence requirements of a modular division conducting operations in the Contemporary Operational Environment (COE). It assesses the nature of the emerging security environment by comparing the U.S. government's strategic and operational threat models with the characteristics of evidentiary threats in the current environment. It poses the question: does the intelligence system of a modular division have the capability to provide a focused and detailed understanding of a networked irregular threat? The diffusion of threats across the globe requires the Army to develop a globally deployable force supported by an intelligence capability with problem specific knowledge. Success with new organizational concepts in the GWOT suggests that commanders must tailor the specialties required to counter the threat to their specific tactical problem. Organizational structure changes within the division can provide the flexibility the Army needs to tailor its divisional intelligence capability to the characteristics of specific threats.

15. SUBJECT TERMS
Intelligence, transformation, terrorism, insurgency, organization theory.

16. SECURITY CLASSIFICATION OF:			17 LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
REPORT	b. ABSTRACT	c. THIS PAGE			19B. TELEPHONE. NUMBER *(Include area code)*
(U)	**(U)**	**(U)**	**(U)**	78	(913) 758-3300

Standard Form 298 (Rev. 8/98)

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

MAJ Frank A. Smith

Title of Monograph: Intelligence Transformation: Comparing Threat Characteristics to Division Capabilities.

Approved by:

_____ Monograph Director
Hugh T. Smith, COL, MI

_____ Director,
Kevin C.M. Benson, COL, AR School of Advanced Military Studies

_____ Director,
Robert F. Baumann, Ph.D. Graduate Degree Programs

Abstract

INTELLIGENCE TRANSFORMATION: USING THREAT CHARACTERISTICS TO DEFINE DIVISION CAPABILITIES by MAJ Frank A. Smith, Army, 78 pages.

The Army's fielding of military intelligence companies to the modular brigade combat teams (BCTs) as part of the Army Transformation has created a loss of intelligence capability for the modular division commander. Furthermore, the global design of the modular brigade and division focus on providing generalist capabilities employable against a wide array of threats and do not favor designing systems that focus on the unique aspects of individual threats. Because predictable intelligence is intent based, it requires a system with capabilities that specialize in the unique aspects of the target adversary.

This monograph explores the intelligence requirements of a modular division conducting operations during the Contemporary Operational Environment (COE). It assesses the nature of the emerging security environment by comparing the U.S. government's strategic and operational threat models with the characteristics of evidentiary threats in the current environment. It poses the question: does the intelligence system of a modular division have the capability to provide a focused and detailed understanding of a networked irregular threat?

The conceptual model of this study is a modular division operating on a non-contiguous battlefield against an irregular, networked threat. By comparing the characteristics of evidentiary and emerging irregular threats to the intelligence system capabilities of a modular division, this study identifies existing intelligence capabilities gaps commanders and planners will need to consider when tailoring force packages for operations in the Global War On Terrorism (GWOT). The purpose of this monograph is to recommend concepts that can mitigate the identified intelligence gaps.

The results of this analysis provide three observations. First, the theoretical threat model the Army is using in its capabilities based approach to force design may be based on a false premise. Second, the capabilities based approach to force design may be insufficient for developing an intelligence organization because intelligence operations are inherently threat specific. Third, the Army must use a mix of matrix, multi-divisional, and functional organizational structures across the intelligence enterprise in order to provide a capability both flexible and knowledgeable.

The diffusion of threats across the globe requires the Army to develop a globally deployable force supported by an intelligence capability with problem specific knowledge. Success with new organizational concepts in the GWOT suggests that commanders must tailor the specialties required to counter the threat to their specific tactical problem. Organizational structure changes within the division and the use of matrix organizations can provide the flexibility the Army needs to tailor its divisional intelligence capability to the characteristics of specific threats.

TABLE OF CONTENTS

TABLE OF FIGURES

CHAPTER ONE

INTRODUCTION

"Honey, someone just flew a plane into the World Trade Center," he heard as he re-entered his apartment. As a certified commercial pilot, he wondered how anyone could be so inept as to pilot a general aviation aircraft into a structure as large as the World Trade Center. He had been downstairs cleaning his mountain bike and his mind was still on the list of things he still had to do before darkness settled in. He was a military intelligence officer preparing to move on Permanent Change of Station orders from Germany back to the United States. At that moment, he came into the living room and witnessed a second airplane strike the World Trade Center on live television. "That was an airliner," he mumbled. "We're under attack." The date was September 11, 2001 and the world had just changed.

This was not the first terrorist attack against the United States, or even against the World Trade Center in New York, but this was the first successful transnational terrorist attack against a domestic U.S. target that resulted in a counteroffensive worthy of the term war. It had two other significant impacts: it resulted in an intelligence reformation act unprecedented in almost 60 years and it galvanized the U.S. Army's most recent effort of organizational change—transformation.

Purpose

This monograph explores the intelligence requirements of a modular division conducting operations during the Contemporary Operational Environment (COE). The Army characterizes the COE as the environment that exists in the world today and will exist until a peer competitor arises.[1] This study assesses the nature of the emerging security environment by comparing the United States government's strategic and operational threat models with the characteristics of

[1] Headquarters, Department of the Army, *FM 2-0: Intelligence* (Washington: GPO, May 2004), 1-23.

evidentiary threats in the current environment. It poses the question: does the intelligence system of a modular division have the capability to provide a focused and detailed understanding of a networked irregular threat?

The conceptual model of this study is a modular division operating on a non-contiguous battlefield against an irregular, networked threat. By comparing the characteristics of evidentiary and emerging irregular threats to the intelligence system capabilities of a modular division, this study will identify existing intelligence capabilities gaps commanders and planners will need to consider when tailoring force packages for operations in the Global War On Terrorism (GWOT). The purpose of this monograph is to recommend concepts that can mitigate the identified intelligence gaps.

Scope

The *National Defense Strategy* (NDS) defines the four challenges emerging in the strategic environment as traditional, irregular, catastrophic and disruptive.[2] This monograph will not examine all of the security challenges identified in the NDS. These are important issues and, ultimately, the modular division must have the capability to counter any of them. This report centers on a networked, transnational, irregular threat. The analytical focus of this monograph is the operational level. In the last decade, many military analysts have written about the strategic level of intelligence reform and military transformation. Few, however, have addressed the linkage between the characteristics of the emerging threat and the organizational structure, skills, and technology the Army needs at the division level to counter this threat. This monograph will begin to bridge that gap by analyzing the intelligence requirements of the modular division confronting an irregular threat to address design issues with its organizational structure.

[2] Headquarters, Department of Defense, *National Defense Strategy of the United States of America* (Washington, DC: GPO, March 2005), 2.

To answer the research question, this study begins by defining the specific military intelligence problem the new geo-political environment presents. It then describes the characteristics of a new threat, categorizes the intelligence capabilities needed to exploit the characteristics of the new threat, and recommends possible solutions to identified shortfalls. This monograph will answer five key questions:

1. What are the fundamental changes in the social, political, and military landscapes?

2. What are the characteristics of a networked, irregular threat?

3. What is the purpose of Army intelligence transformation?

4. What capabilities does the intelligence system of a modular division need to counter a networked, irregular threat?

5. What are the gaps between the characteristics of the threat and the design characteristics of a modular division's intelligence system?

The results of this analysis provide three observations. The theoretical threat model the Army is using in its capabilities based approach to force design may be based on a false premise. The modern, irregular threat may have chosen its organizational structure and asymmetric tactics for proactive, not reactive reasons. Some have stated that U.S. dominance in conventional warfare has forced the emerging threat to choose a networked organizational structure and asymmetric tactics. It assumes the threat would prefer to form a conventional army and conduct conventional warfare, but it cannot afford to solely because of the associated tactical risks. The characteristics of the contemporary environment support a competing hypothesis. The modern, irregular threat may prefer a networked organizational structure and set of asymmetric tactics for proactive, not reactive, reasons.

Second, the capabilities based approach to force design may be insufficient for developing an intelligence organization because intelligence operations are inherently threat specific. General intelligence capabilities only provide limited understanding of adversaries. Capabilities that provide insight into the specific social, political, religious, cultural, and military

aspects of a given threat are critical to a complete intelligence estimate. The goal of Army intelligence is to provide intent based predictive intelligence. This requires information specific to the targeted adversary.

Third, the Army must use a mix of matrix, multi-divisional, and functional organizational structures across its intelligence activities in order to provide a capability that is both flexible and knowledgeable. The diffusion of threats across the globe requires the Army to develop a globally deployable force supported by an intelligence capability with problem specific knowledge. Success with organizations such as the Joint Inter-Agency Task Force (JIATF) suggests that commanders must tailor the specialties required to counter the threat to their specific tactical problem. Organizational structure changes within the division and the use of matrix organizations can provide the flexibility the Army needs to tailor its divisional intelligence capability to the characteristics of specific threats.

What is the specific military problem?

Recent shifts in the geo-political environment since the demise of the Soviet Union have created a specific military problem. During the Cold War, the United States focused on one threat, the Soviet Union, and considered all other threats as lesser-included contingencies. As noted in a study on transformation prepared for the Secretary of Defense in April 2001, "The overriding priorities during the Cold War were a clear capability to (1) deter a nuclear attack against the United States and its allies; (2) deter war between superpower coalitions; and (3) if deterrence failed, ensure marginal superiority over Cold War opponents sufficient to assure that a conflict would be resolved on terms favorable to the United States and its allies."[3] A stable,

[3] Headquarters, Department of Defense, Transformation Study Group, *Transformation Study Report Executive Summary: Transforming Military Operational Capabilities,* (Washington: 27 April 2001), 1. The Secretary of Defense convened the Transformation Study Group on March 5, 2001. The Secretary of Defense charged the group to identify capabilities needed by U.S. forces to meet the challenges of the twenty-first security environment, capabilities needed to meet national intelligence and space defense

peaceful world order did not emerge from the aftermath of the Cold War. Instead, four challenges emerged that threaten U.S. interests across the globe. These challenges are transnational irregular threats, the proliferation of weapons of mass destruction and ballistic missile technology, and the increasing conventional capabilities of regional powers. Because of the increase in numbers and types of threats, the Army can longer afford to focus on defeating one type of threat. It can no longer assume that preparing for a peer conflict is the most dangerous eventuality and that preparing for it will provide the capabilities needed for the other security challenges. Instead of a regionally focused military centered on a Soviet threat model, the Army is now transforming into a global expeditionary force. The shift from a bi-polar geo-political environment to a multi-polar environment has necessitated a change in the Army force design.

The military intelligence system developed for the Cold War lacks the capabilities required to counter the characteristics of the emerging threats. Perhaps more than during the Cold War, operational success depends on the intelligence system providing the commander with expert knowledge of the political, cultural, social, economic, and military nuances of the emerging threats. Of the four challenges, the modern irregular threat is the most demanding in this sense. This threat is an urbanized, networked, irregular force that is willing to use terrorism on a massive scale as a means of strategic attack in order to attain its political ends. A sophisticated adversary, it is adept at leveraging information and technology to influence regional and global opinion. The intelligence capability of the modular division must be able to understand and exploit more than the adversary's military source of power. Intelligence must be knowledgeable across the critical dimensions of the operational environment.

---

needs, transformation recommendations, and opportunities for cost savings. This paper summarizes a report presented to the Secretary of Defense in the form of briefing charts on April 27, 2001.

The specific military intelligence problem is balancing the tension between the need to deploy globally with the requirement to understand detailed aspects of each emerging adversary. The modular division does not have the organic capability to understand the cultural, social, political, and military nuances of any specific emerging threat because the Army leadership has specifically designed it for global, rather than regional, employment. The modular division's intelligence capability must be integrated and interoperable with the national intelligence enterprise. The national intelligence enterprise includes not only Department of Defense agencies and organizations, but represents the entire set of national intelligence activities. To counter the emerging irregular threats, modular divisions require a tailored intelligence capability that combines the flexibility and responsiveness of organic intelligence assets with the specificity and expertise of regionally focused assets at theater and national level.

CHAPTER TWO

WHY ORGANIZATIONS CHANGE

Organization theory provides the analytical framework of the Army's intelligence capabilities. A full discussion of organization theory is beyond the scope of this monograph. However, an analysis of the organizational structure of the modular division, the Army intelligence system, and the threat is essential to understanding the benefits and drawbacks the various structures provide. This report uses Mary Jo Hatch's framework for organizational structure from her work *Organization Theory.* Appendix A contains a brief description of the organizational structures used in the study. Readers who have a limited background in organization theory may wish to review this information to gain a better understanding of the analysis of the modular division's intelligence capability.

Change and organizational structure

Hatch categorizes the various organizational structures into groupings of similar characteristics and identifies six (6) forms of organizational structure: simple, functional, multi-divisional, matrix, hybrid, and networked. Each of these structures has distinct hierarchy, authority, and division of labor characteristics as demonstrated in figure 1. Hierarchy reflects the distribution of authority among organizational positions. Authority grants the position holder certain rights including the right to give direction to others and the right to punish and reward. Division of labor defines the distribution of responsibilities.[4]

[4] Mary Jo Hatch, *Organization Theory* (New York: Oxford University Press, 1997), 164-165.

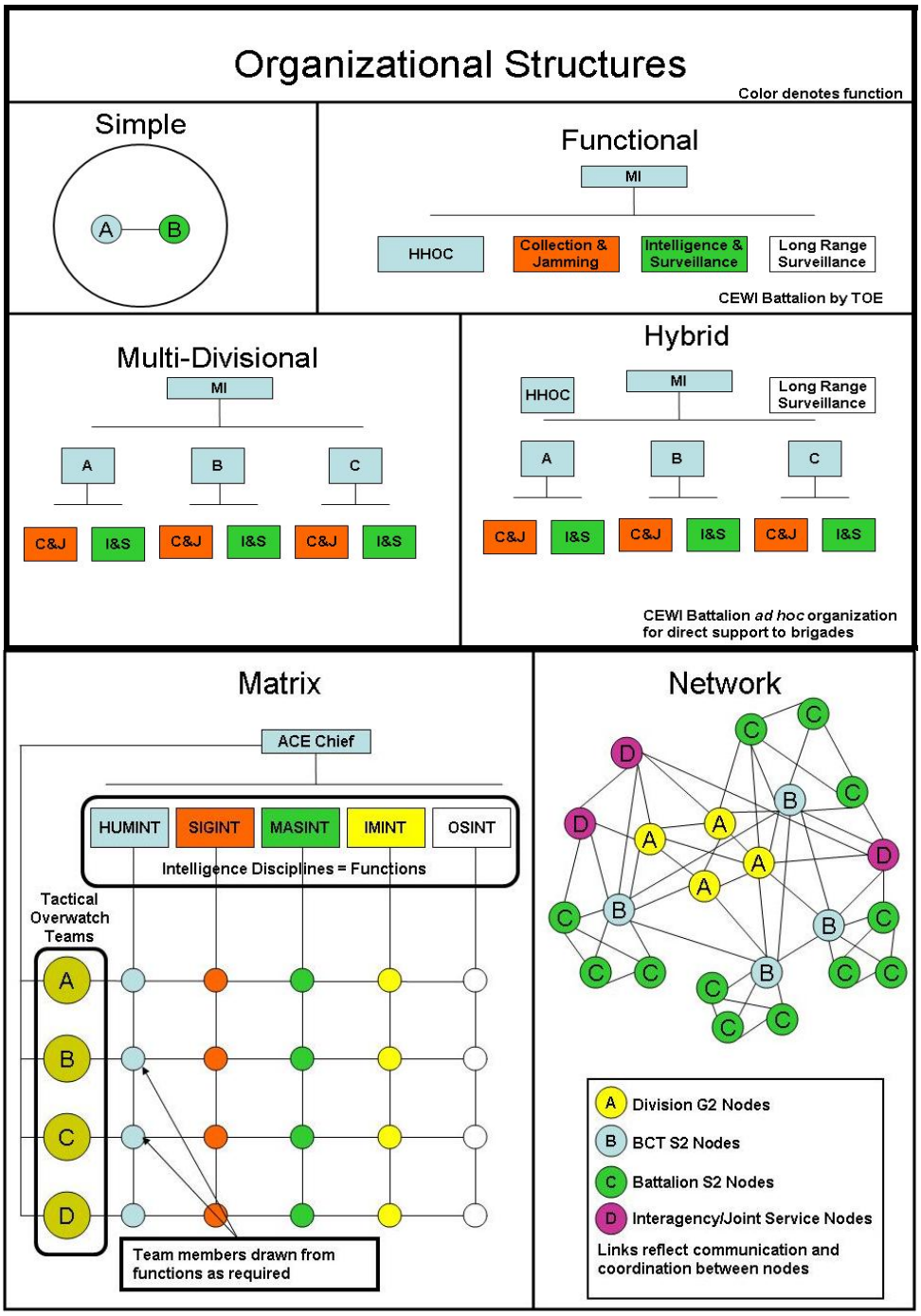

Figure 1: Organizational structures of generic military intelligence systems.

Adapted from categories described in Mary Jo Hatch, *Organization Theory* (New York: Oxford University Press, 1997), 182-192.

In the Army, command and support relationships define the authority and division of labor responsibilities for its organizations. FM 3-0, *Operations* states, "Commanders build combined arms organizations using command and support relationships. Command relationships define command responsibility and authority. Support relationships define the purpose, scope, and effect desired when one capability supports another."[5] This monograph will use the definitions contained in FM 3-0, *Operations* in its analysis of the modular division.

The intelligence system within a modular division is an organization. An organization is "any unified, consolidated group of elements; systematized whole; especially, a body of persons (formed together) for some specific purpose."[6] Organizations include the "technologies, social structures, cultures, and physical structures that overlay and interpenetrate one another within the context of an environment."[7] Leaders use specific organizational structures to facilitate the organization's ability to perform its designed functions. Organizational leaders change the organization's structure when it does not perform the designed functions to expectations, when modifications of process increase the organization's ability to perform its functions, or when changes in the external environment require a change in the specified functions of the organization. Improving the Army's intelligence system is one of the Army Chief of Staff's top priorities within the context of Army Transformation. One of the most dramatic changes in Army Transformation is the change of organizational structure to the intelligence system within a division.

The Department of Defense Transformation Planning Guidance (TPG) states, "Transformation is necessary to ensure U.S. forces continue to operate from a position of overwhelming military advantage in support of strategic objectives. We cannot afford to react to

---

[5] Headquarters, Department of the Army, *FM 3-0: Operations*, (Washington: GPO, June 2001), 4-29.

[6] *Webster's New Universal Unabridged Dictionary, Second Edition* (1983), s.v. "organization" and "organize."

[7] Hatch, 15.

threats slowly nor have large forces tied down for lengthy periods."[8] In order to achieve this position of advantage, the Army should seek to maximize the utilization of its intelligence specialists. The TPG continues, "Today we are witnessing the transition from the industrial age, with its emphasis on mass, to the information age where the power of distributed networked forces and shared situational understanding will transform warfare."[9]

The hierarchical organizational structure of the Army evolved from industrialism. In the mid to late 1800s, manufacturers spread the use of the factory system to clothing and food manufacturing. The increased technical complexity of manufacturing operations "demanded parallel growth in systems of social organization and bureaucracy, with their emphasis on control, routine, and specialization."[10] Other fields such as engineering, metal processing, and national armies turned to the factory system to gain similar efficiencies.

Hatch notes that whereas industrial societies organize around the control of labor in the production of goods, post-industrial society organizes around the creation of knowledge and the uses of information. A central aspect of the post-industrial era, or the information age, is the revolution in computing technologies and subsequent globalization of world markets. This information revolution is allowing organizations to depart from the industrial era hierarchical organizational structure in favor of more horizontally structured organizations because they can share information almost instantaneously.[11]

[8] Headquarters, Department of Defense, *Transformation Planning Guidance* (Washington: GPO, April 2003), 4.
[9] Ibid., 5.
[10] Hatch, 23
[11] Ibid., 24.

Army intelligence is a system

Army intelligence is a complex adaptive system. Organizations are complex adaptive systems if they react to variations in their environment and seek change in order to survive.[12] Robert Axelrod and Michael D. Cohen provide a thorough discussion of systems and complexity in their book *Harnessing Complexity*. Their definitions and framework provide the bridge that joins the analysis of why the Army is changing to how the Army is changing in this study. This framework also provides a common language for the analysis of the Army intelligence system within a modular division. Appendix B includes a general overview of Axelrod's framework and definitions.

The intelligence capability of a modular division is a complex adaptive system because it seeks to adapt to changes in its environment. An example of this is evident in the opening remarks of the *2004 Army Transformation Roadmap* that states:

> The Army is transforming for continuous operations as a campaign-quality Army with joint and expeditionary capabilities. This new strategic reality is defined by: a conflict of irreconcilable ideas, a disparate pool of potential combatants, adaptive adversaries seeking our destruction by any means possible, evolving asymmetric threats that will relentlessly seek shelter in those environments and methods for which the nation is least prepared, (and) a foreseeable future of extended conflict in which the Army can expect to fight every day and in which real peace will be the anomaly.[13]

Through transformation, Army leadership is intervening in the Army system by issuing changes to their strategy and re-ordering the Army's capabilities in order to adapt to a changing strategic environment. The intelligence capability of a modular division, as a subsystem of the Army, is also a complex adaptive system. In conjunction with the actions of the Army leadership, the military intelligence leadership is intervening in its subsystem by changing its strategy and re-ordering its capabilities to adapt to the changing strategic environment.

---

[12] Robert Axelrod and Michael D. Cohen, *Harnessing Complexity* (New York: Basic Books, 2000), 7.

[13] Headquarters, Department of the Army. *The 2004 Army Transformation Roadmap*. (Washington, DC: GPO, July 2004), 1-1.

Army intelligence is also an open system. An open system receives inputs from its environment and transforms them into outputs. It relies on its environment for its survival.[14] In this case, the external environment provides the purpose for the system in the form of a threat force acting against U.S. national interests. The threat provides the inputs as indicators that the intelligence system converts, or transforms, into outputs of intelligence information for the commander, or an understanding of the operational environment.

Understanding the Army intelligence capability as a complex adaptive system helps conceptualize the impact changes have across echelons. The national intelligence enterprise is a set of embedded systems. The modular division's intelligence system is an open subsystem in the national intelligence enterprise. Its super system is the theater army's intelligence capability inclusive of all analysis and collection assets subordinate to a numbered Army. The subsystems within the modular division include the analysis and collection capability that is organic to the division G-2, Brigade Combat Teams (BCTs), and support brigades, especially the Battlefield Surveillance Brigade (BFSB). Each of these systems has an organizational structure that provides certain strengths and weaknesses to the division's aggregate intelligence capability.

Army Transformation is more than transformation

Change is not new to the Army. It is a continuous process in any organization that competes for survival. However, the types of changes within the Army shift depending on changes in its internal and external environments. To categorize these changes and maintain a common understanding with the reader, this monograph will use familiar definitions from *Webster's New Universal Unabridged Dictionary* for four types of change: reformation, modernization, recapitalization, and transformation. The distinction may seem trivial, but a clear

[14] Hatch, 38.

understanding of these terms is critical to understanding the complexity of the organizational change within the Army intelligence community.

Reformation is a correction of faults.[15] It is change that addresses organizational deficiencies. Recently many authors have written on the subject of intelligence reform and their topics are consistent with this definition. In the wake of the 11 September 2001 attacks, Congress initiated a broad sweeping review of the national intelligence system that resulted in the first major adjustment to intelligence legislation since the National Security Act of 1947. The Intelligence Reform and Terrorism Prevention Act of 2004 changed the organizational structure of the national intelligence system, created the office of the Director of National Intelligence, and addressed the institutional deficiency of information sharing between agencies by bridging the legislated divide between domestic and foreign intelligence activities.[16]

Modernization involves the employment recent techniques, methods or ideas.[17] Organizations modernize to gain efficiency, reduce risk, and reduce costs. By adopting technological advances or improvements in process, organizations seek an advantage over their competitors. The Army modernizes its systems on a continuous basis to ensure capability overmatch against its potential adversaries and to reduce risk exposure to its soldiers. Fielding equipment variants and introducing new technologies are modernization activities. The use of Unmanned Aerial Vehicles (UAV) is a modernization of aerial reconnaissance. It improves the ability of Army units to conduct aerial reconnaissance and surveillance while reducing the overall cost of the activity and risk to soldiers.

---

[15] *Webster's New Universal Unabridged Dictionary, Second Edition* (1983), s.v. "reformation"

[16] Michael Warner, "Intelligence Transformation: Past and Future," in *Rethinking the Principles of War,* ed. Anthony D. McIvor (Annapolis: Naval Institute Press, 2005), 519, 522-523.

[17] *Webster's New Universal Unabridged Dictionary, Second Edition* (1983), s.v. "modernization."

Recapitalization is changing the capital structure of an organization.[18] An organization recapitalizes when it changes the priorities of its capital allocations among its competing internal demands. The Army recapitalizes when it decides to stop funding certain activities, or fund them at a lower level, in order to increase funding to another activity. The termination of the Comanche helicopter program and reallocation of its resources to other projects is an example of recapitalization.

Transformation is a change in condition, nature, or function. It is a conversion from one state to another.[19] Transformation describes the change an organization undergoes when it changes its core competencies or essential products or services. The Army transforms when it institutionalizes a new capability or competency in order to adapt to changes in the demands of the external environment.

The Department of Defense uses the term transformation to describe these four types of change in one set. The Department of Defense *Transformation Planning Guidance* defines transformation as "a process that shapes the changing nature of military competition and cooperation through new combinations of concepts, capabilities, people and organizations that exploit our nation's advantages and protect against our asymmetric vulnerabilities to sustain our strategic position, which helps underpin peace and stability in the world."[20]

Transformation is a continuous process by the military to ensure it provides the skills and abilities necessary to counter threats if the Department of Defense views the strategic environment as ever-changing. In this context, Defense Transformation, and subordinately Army Transformation, is the entire set of changes that reform, modernize, recapitalize, and transform the military's capabilities in order to adapt continuously to a changing strategic environment.

---

[18] Ibid., s.v. "recapitalization."
[19] Ibid., s.v. "transformation."
[20] Headquarters, Department of Defense, *Transformation Planning Guidance* (Washington: GPO, April 2003), 3.

Transformation, innovation, and revolutions in military affairs

Some argue that these changes are not continuous, but periodic. Supporters of this view believe that these periods of innovation represent the military's effort to adapt to fundamental changes in social, political, and military landscapes. They call this a revolution in military affairs. Proponents of this view argue there are two separate and distinct phenomena that drive change in the military: the military revolution and the revolution in military affairs (RMA). Allan R. Millett and Williamson Murray suggested as a hypothesis in their book *Military Innovation in the Interwar Period*, "We are now in the early stages of a period in which advances in precision weaponry, sensing and surveillance, computational and information-processing capabilities, and related systems will trigger substantial changes in future wars, changes at least as profound and far reaching as combined-systems "revolutions" of the interwar period."[21]

The authors contend that the world has experienced five (5) military revolutions.[22] Whether or not the U.S. Army is in the midst of a sixth military revolution continues to be open to debate and the answer to that question is certainly beyond the scope of this paper. However, the framework Murray used in his study is useful in understanding the changes occurring externally in the geo-political environment and internally in the Army and the Military Intelligence Corps specifically.

---

[21] Williamson Murray and Allan R. Millett, eds., *Military Innovation in the Interwar Period*, (Cambridge: Cambridge University Press, 1996; Cambridge, 1998), 405.

[22] MacGregor Knox and Williamson Murray, eds., *The Dynamics of Military Revolution, 1300-2050*, (Cambridge: Cambridge University Press, 2001; reprint, New York: Cambridge University Press, 2003), 6-11 (page citations are to the reprint edition). The authors contend that the first military revolution was the creation in the 17th century of the nation-state because it produced large-scale organization of disciplined military power. The second military revolution was the French Revolution because it merged mass politics and warfare. The third military revolution was the Industrial Revolution because industrialization enabled states to arm, clothe, feed, pay, and move mass armies. World War I was the fourth military revolution because it combined the merging of mass politics and warfare from the French Revolution and the mass production and transportation changes of the Industrial Revolution, which set the pattern for 20th century warfare. Finally, he argues that the advent and use of nuclear weapons was a military revolution because it deterred war through mutually assured destruction.

In *Dynamics of Military Revolution,* Murray defines a military revolution as a phenomenon that fundamentally changes the framework of war. A military revolution results from massive social and political changes that forces societies and states to restructure and fundamentally alters the manner in which military organizations prepare for and conduct war.[23]

An RMA is a period of innovation in which armed forces develop novel concepts involving changes in doctrine, tactics, procedures, and technology. They are clusters of less all-embracing changes that appear to be susceptible to human direction. He contends that these phenomena almost exclusively take place at the operational level of war and always occur within the context of politics and strategy. They are the military's effort to adapt to fundamental changes in social, political, and military landscapes. RMAs emerge from evolutionary problem solving directed at specific operational and tactical issues in a specific theater against a specific enemy. They require a complex mix of tactical, organizational, doctrinal, and technological innovations.[24]

Murray contends that innovation within the military is complex in nature; it is non-linear and displays extreme sensitivity to current and initial conditions.[25] Innovations in Murray's context of an RMA are the artifacts agents use to place interventions in to specific subsystems of the Army to produce changes the leadership desires. Axelrod defines systems as complex "when there are strong interactions among its elements, so that current events heavily influence the probabilities of many kinds of later events."[26] This corresponds with Murray's observation that the process of innovation is non-linear and extremely sensitive to current and initial conditions.

Current changes in the military intelligence capabilities of a modular division may be part of an RMA as Murray defines it. This period is certainly a time in which the Army is adapting to

---

[23] Ibid., 7.
[24] Ibid., 176, 179-180.
[25] Ibid., 12. and Murray and Millett, eds., *Military Innovation in the Interwar Period,* 302-303.
[26] Axelrod and Cohen, 7.

meet the changes in the social, political, and military landscapes and it is doing so with a mix of tactical, organizational, doctrinal, and technological innovations that demonstrate complex interactions within the Army intelligence system.

Although the Army intelligence system is changing, it is not transforming. It is not converting its core competency or essential service into a different core competency or essential service. It does not have a new purpose. Army intelligence is modernizing, reforming, and recapitalizing in order to best utilize finite resources. It is innovating to adapt current processes and discover new processes that improve its ability to fulfill its purpose, to provide the commander with an understanding of his adversary.

CHAPTER THREE

THE PURPOSE OF ARMY INTELLIGENCE

The purpose of Army intelligence remains constant, but the capabilities required to achieve the purpose have changed. The purpose of intelligence is to provide the commander with an understanding of the adversary and the environment in order to facilitate his operational decisions. The Army intelligence system in use today is obsolete because the Army designed it to counter a specific threat, the Soviet Union, that no longer exists and no similar competitor replaced it. The personnel and equipment developed during the Cold War were not generalist in nature, but very specific to the threat. Therefore, because the threat has changed, the capabilities of Army intelligence must also change. The Army must produce experts in the new threat's characteristics and develop capabilities focused on exploiting the new threat's systems in order to understand it.

The role of intelligence

Joint Publication 1-02, The Department of Defense Dictionary of Military and Associated Terms, defines intelligence as "the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas" or "information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding."[27] The national intelligence system is a complex system of interdependent organizations that are responsible for collecting and analyzing the global environment to provide leaders this information. The role of the American intelligence system is to provide national civilian and military leaders with information about potential adversaries and environmental conditions that they need in order to make decisions.

[27] Headquarters, Department of Defense, *JP 1-02: DOD Dictionary of Military and Associated Terms* (Washington: GPO, 12 April 2001, as amended through 31 August 2005), 266.

The Army intelligence system is a subsystem within the Joint intelligence system, which resides within the larger national intelligence enterprise. The purpose of Army intelligence is to provide an understanding of the enemy to assist in the planning, preparation, and execution of military operations. It assists the commander in visualizing his battlespace by providing predictive assessments of enemy capabilities and intentions.[28]

The organization of Army intelligence

The Army categorizes its capabilities into seven Battlefield Operating Systems (BOS). The BOS are functional groupings of capabilities that enable commanders to build, employ, direct, and sustain combat power. The functional group that describes the Army's intelligence capability is the Intelligence Battlefield Operating System (IBOS). The IBOS is a complex set of organizations, people, and equipment that operates worldwide, across strategic, operational, and tactical domains.[29]

The IBOS represents a unified grouping formed together for a specific purpose, an organization. It reacts to variations in its environment; it is an adaptive system. It consists of more than the traditional intelligence assets organized under the military intelligence branch: it includes any asset capable of conducting intelligence, surveillance, and reconnaissance (ISR) operations. The IBOS consists of four functions: collecting, processing, analyzing, and delivering intelligence.[30] A wide array of ISR assets covering seven major disciplines reside within these functions.

ISR is "an enabling operation that integrates and synchronizes all battlefield operating systems to collect and produce relevant information to facilitate the commander's decision

[28] Headquarters, Department of the Army, *FM 2-0: Intelligence.* (Washington: GPO, 17 May 2004), 1-1, 1-2.
[29] Ibid., 1-2.
[30] Ibid., 1-3.

making."[31] ISR assets are "those organizations, systems, sensors, personnel, and equipment dedicated to or directed toward the collection of information in response to the commander's critical intelligence requirements."[32] Therefore, any asset the commander tasks to collect information about the adversary or the environment is an ISR asset. Every soldier and every piece of gear could be included in this grouping. Therefore, to scope the analysis of the modular division, this research will only consider those organizations, personnel, equipment, and systems that primarily fulfill an intelligence discipline by design.

An intelligence discipline is "a well defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. The seven major disciplines are human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, open-source intelligence, technical intelligence, and counterintelligence."[33] The seven disciplines provide information about the adversary and expertise that informs the analysis of that information. However, commanders need an understanding of the adversary, not just information. The intelligence organization gains an understanding through the analysis and fusion of the information the disciplines provide. The national expectation of these seven disciplines is to provide timely warning of pending attack and accurate target information for military operations. However, the history of the nation's intelligence program establishes significant barriers to the development of an integrated, interdependent intelligence enterprise that impact down to the tactical echelon.

[31] Headquarters, Department of the Army, *FM 1-02: Operational Terms and Graphics*, (Washington: GPO, September 2004), 1-102.

[32] Ibid., 1-102.

[33] Headquarters, Department of Defense, *JP 1-02: DOD Dictionary of Military and Associated Terms* (Washington: GPO, 12 April 2001, as amended through 31 August 2005), 266.

How has intelligence changed over time?

The modern national intelligence system developed from a shift in the national strategy as the United States entered World War I. During the war and immediately following it, the nation's grand strategy shifted from isolationist commercial neutrality to active global engagement. Although much of the world retreated into closed economies after the devastation of World War I, American companies were in a unique position to expand their overseas investments and expand their markets because they were relatively unaffected by the war.[34] This increased the globalization of the American economy while the increased range and lethality of the new air and sea borne weapons simultaneously began to challenge the geographic safety the oceans provided the United States.[35] These challenges created a need for four intelligence missions that continued to evolve through the Second World War and post war period: homeland defense, clandestine activities abroad, support to military operations, and support to the president.[36]

The National Security Act of 1947 codified these emerging missions, but deliberately did not unify the nation's intelligence efforts. Concern over the protection of civil liberties for American citizens led to compromises in the legislation that divided the U.S. intelligence efforts. It established separate organizations for internal and external security and intelligence missions, allowed for military control of its own intelligence operations by service, and established the Central Intelligence Agency independent of the military services.[37] The legislation led to an organizational division of effort that separated U.S. intelligence efforts along domestic and foreign lines and national-political, law-enforcement, and military lines.

---

[34] IMF Staff, "Globalization: Threat or Opportunity?" International Monetary Fund Website, April 12, 2000 (Corrected January 2002), accessed from http://www.imf.org/external/np/exr/ib/2000/041200.htm.

[35] Michael Warner, "Intelligence Transformation Past and Future," in *Rethinking the Principles of War*, ed. Anthony D. McIvor (Annapolis: Naval Institute Press, 2005), 517.

[36] Ibid., 518.

[37] Ibid., 519-520.

The National Security Act of 1947 remained in effect as the broad guidance governing intelligence affairs until the passage of the Intelligence Reform and Terrorism Prevention Act of 2004. This legislation changed the organizational structure of the national intelligence system, created the office of the Director of National Intelligence, and addressed the institutional deficiency of information sharing between agencies. It began to bridge the legislated divide between domestic and foreign intelligence activities.[38]

The organizational structure of the Army's intelligence capability has held many forms since the establishment of the 1947 legislation. A complete review of the history of the Army's intelligence systems and the military intelligence branch is beyond the scope of this monograph. However, it is significant to note that the Army has changed the organizational structure of its intelligence capability multiple times over the past half century as it struggled with the tension between limited resources and shifting capability demands. The development of one organization demonstrates the Army's efforts to improve its effectiveness by modifying its organizational structure. It is the Combat Electronic Warfare and Intelligence (CEWI) battalion.

The CEWI battalion marked the first time Army leaders supported an intelligence organization organic to the division. In both 1957 and 1962, the Army considered organic intelligence units at the division level and rejected them because of unaffordable overhead and challenges with resource allocation. One of the greatest resource challenges was the allocation of appropriate linguists because of the variations required across the Army's potential theaters.[39]

The Army developed the CEWI battalion concept based on recommendations from the 1975 Intelligence Organization and Stationing Study. The 2nd Armored Division at Fort Hood fielded the first CEWI battalion, the 522nd Military Intelligence Battalion, in 1976.[40] The first

[38] Ibid., 519, 522-523.

[39] John Finnegan and Romana Danysh, *Military Intelligence* (Washington, D.C.: United States Army Center of Military History, 1998), 179.

[40] Ibid., 179-180.

Table of Organization and Equipment for the CEWI battalion appeared in 1979. It authorized a headquarters and headquarters and operations company (HHOC) and three line companies. The HHOC contained the collection management, counterintelligence, and interrogation capabilities, and had a platoon of helicopters equipped for electronic missions. The battalion's three line companies had functional organizational structures. One company conducted collection and jamming of radio signals, a second conducted ground surveillance with radar and sensors, and a third company provided service support. Within ten years, the battalion also gained a long-range reconnaissance capability.[41] This organizational structure provided benefits in training and resource oversight, but hindered its effectiveness during tactical employment.

Although the CEWI battalion provided intelligence assets in general support the division commander, the formal organization did not allow for direct support to the subordinate brigade commanders. Often unit commanders would use command and support relationships to develop three *ad hoc* company teams containing elements of each discipline to support the needs of the brigade commanders. Matrix organizations such as this can create a conflict in authority. Because the soldiers belong to the functional structure, but work for the *ad hoc* structure, they can experience stress from the competing demands of the two supervisors.[42] It dilutes unity of command. In this organization, the soldiers of a military intelligence company had the potential of being responsible to four different leaders. They were directly responsible to their functional company commander and their *ad hoc* company team commander and they were indirectly responsible to the military intelligence battalion commander and the maneuver brigade commander.

Army transformation attempts to address these challenges. It recognizes that shifts in the geo-political environment require changes in the capabilities of its intelligence system. It

[41] Ibid., 180-181.
[42] Hatch, 189.

recognizes the strengths and weaknesses of these historical organizational structures and it realizes that it must balance the tension between limited resources and increasing capabilities requirements. Only by determining the characteristics of the new operational environment can the Army adequately design its intelligence capability.

CHAPTER FOUR

THREAT MODELS OF THE CONTEMPORARY OPERATIONAL ENVIRONMENT

Fundamental changes in the social, political, and military landscapes that emerged since the end of the Cold War demand dramatically influence the United States' approach to strategic, operational, and tactical problems including the force design requirements for Army intelligence. This chapter identifies the shifts in the adversarial forces that oppose U.S. national interests, defines the four categories of challenges to national security that the Department of Defense and Army leadership are using to frame the new strategic environment, and evaluates three threat models used by the U.S. government. It centers on a specific threat in this new strategic environment that is driving intelligence transformation, the transnational irregular threat.

Fundamental changes

A bipolar balance of power between two politically diverse nation-states defined the strategic environment of the 20th century. Today multi-polarity defines the global strategic environment. Regional disputes over ideology, religion, race, and resource control will foment conflicts in the coming years. It is probable that parties instigating these conflicts will target the United States and its interests abroad. They will most likely use irregular methods of warfare to circumvent U.S. dominance in traditional warfare. The future irregular adversary will probably exploit existing communication and transportation infrastructures and commercial technologies provided by globalization to strike at the very heart of the United States, its people.

In the *2001 Quadrennial Defense Review Report*, the Department of Defense identified this fundamental shift in the threat facing the United States. It stated:

> Unlike the Cold War period, where the key geographic regions of competition were well defined, the current period has already imposed demands for U.S. military intervention or activity on virtually every continent and against a wide variety of adversaries. The United States will not be able to develop its military forces and plans solely to confront a specific adversary in a specific geographic area. Instead, the United States could be forced to intervene in unexpected crises against opponents with a wide range of

> capabilities. Moreover, these interventions may take place in distant regions where urban environments, other complex terrain, and varied climatic conditions present major operational challenges.[43]

Written eleven years after the fall of the Soviet Union, this statement captures the complexity emerging in the global strategic environment throughout the 1990s. During the Cold War, the United States and the Soviet Union maintained a precarious balance of power and with it a relative state of regional stability. The overriding U.S. policy was containment.[44] Regional conflict was limited to proxy wars as the two superpowers vied for the control of states and resources. Unlike the early 20th century, the proxy wars did not develop into global conflict because of the threat of a nuclear exchange between the superpowers.

With the loss of a second superpower, regional powers found themselves freed from their Cold War restraints. Underlying currents of ethnic, religious, economic, and political tension began to surface. Enabled by a globalized market, military capability spread quickly as cash strapped failing states liquidated their conventional military stocks and regional state and non-state powers expanded their unbridled military, informational, and economic forces. Some states fragmented along these social lines and regional conflict ensued. Authors such as Samuel Huntington, John J. Mearsheimer, and Thomas P.M. Barnett, and agencies such as the International Monetary Fund (IMF) have written extensively on this topic and are a valuable source for further background.[45] Across the literature, one emerging trend stands out: the

---

[43] Headquarters, Department of Defense, *Quadrennial Defense Review Report* (Washington: GPO, September 2001), 6.

[44] *NSC 68: United States Objectives and Programs for National Security* (April 14, 1950), Section VI: U.S. Intentions and Capabilities—Actual and Potential, A: Political and Psychological. Accessed online at http://www.mtholyoke.edu/acad/intrel/nsc-68/nsc68-1.htm.

[45] Samuel Huntington, *The Clash of Civilizations,* (New York: Touchstone Books (Simon & Schuster, Inc.), 1997), 42-44, 125, 135, and 207-218 discusses the fissure of regional stability along civilization lines. John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W. W. Norton, 2001) 2-3, centers his argument on a nation's perpetual pursuit of power to enhance its security. IMF Staff, "Globalization: Threat or Opportunity?" International Monetary Fund Website, April 12, 2000 (Corrected January 2002), accessed from http://www.imf.org/external/np/exr/ib/2000/041200.htm, Thomas P.M. Barnett, "The Pentagon's New Map," *Esquire*, March 2003 and Thomas P.M. Barnett and Henry H. Gaffney, Jr. "The Global Transaction Strategy," *Military Officer*, May 2003, accessed online

emergence of a violent transnational social movement founded on fundamentalist interpretations of Islam. Huntington has characterized this type of movement as an inter-civilization conflict.[46]

Inter-civilization conflict takes two forms. At the micro level, fault line conflicts occur between neighboring states from different civilizations, between groups from different civilizations without a state, and between groups that are attempting to create new states out of failed states. At the macro level, core state conflicts occur among the major states of different civilizations. One conflict between civilizations emerging is between fundamental Islam and the secular West. Causes of this conflict flow from the nature of the two religions and the civilizations based on them. Factors that increase the conflict between these two civilizations are population growth, Islamic resurgence, the west's efforts to universalize its values and institutions, the collapse of communism, and increasing contact between Muslims and westerners.[47] This is an example of a macro-level inter-civilization conflict; however, there are also micro-level conflicts within Islam such as the disparity between Shi'ia and Sunni interpretations and the disparity between fundamental and moderate interpretations of Islam. This type of conflict signifies a critical shift in the operational environment. States fought Cold War conflicts to resolve disputes in political ideologies. State and non-state actors are fighting contemporary conflicts to resolve disputes in religious ideologies.

The resulting geo-political environment is significantly different from that of the Cold War. Instead of bi-polar, it is multi-polar. Instead of being politically centric, it is oriented on religious, ethnic, and cultural schisms. Instead of producing a stabilizing effect between superpowers, weapons of mass destruction and effect are now the tools of individuals and non-state actors, which they can use to hold nations hostage.

---

http://www.thomaspmbarnett.com, address the affects of globalization on developed and underdeveloped states.

[46] Huntington, 207.

[47] Ibid., 207-208, 209-218.

The National Model: four security challenges

Government and military sources provide three models that use a capabilities-based approach to describe the threat in the contemporary geo-political environment. They are the national model, as described in U.S. policy and strategy documents; the joint model, as described in joint doctrine and concept papers; and the Army model, as described in Army doctrine and concept papers. As conceptual representations of the contemporary environment, these models do not identify capabilities of specific evidentiary threats, but consider the range of capabilities any adversary could reasonably employ against the United States. Instead of focusing on *who* threatens the United States, they focus on *how* an adversary could threaten the United States.

The national leadership identified the shift in the strategic environment and captured it in its national strategies and security estimates. The *Quadrennial Defense Review Report* formalized this shift in global perception in 2001. It concedes, "An assessment of the global security environment involves a great deal of uncertainty about the potential sources of military threats, the conduct of war in the future, and the form that threats and attacks against the Nation will take."[48] Despite this uncertain environment, the report suggests that the Department of Defense can learn from current geo-political and military technical features and trends in the current environment to shape the capabilities it will need in the near future.[49]

Unlike the ideologically defined political blocs of the Cold War, the new geopolitical and military-technical trends center on the increasing fluidity in the international system and the uncertainty it creates. The diffusion of political power combined with the proliferation of military and information technology has increased the United States' vulnerability to domestic attack. During the Cold War, the United States was vulnerable to Soviet missile attacks, but it developed the political, military, and technological capabilities to monitor, dissuade, and deter

[48] Headquarters, Department of Defense, *Quadrennial Defense Review Report* (Washington: GPO, September 2001), 3.

[49] Ibid., 3.

Soviet nuclear aggression. These Cold War capabilities are less effective against the multiple threats in the more fluid international system.[50]

While recognizing that any weak or failing state can destabilize a region and endanger U.S. interests, the QDR report identifies three regions that are of particular concern to the United States: Asia, the Andean region, and the area that stretches from the Middle East to Northeast Asia that the report describes as the "Arc of Instability." Weak and failing states in these regions could facilitate the operations of transnational threats. Challenges resulting from weak state government in these regions include state sponsorship of terrorism, provision of sanctuary in large ungoverned spaces, and access to weapons of mass destruction and effects and other military technology. An increase in the proliferation of ballistic missile technology and weapons of mass destruction and effects combined with the increase in travel and trade across the United States' borders decreases the security the United States' geographic separation provided during the Cold War. Conversely, the vast distances of these regions combined with current access restrictions and limited existing bases could severely limit the United States' ability to respond to an attack on its national interests.[51]

To address the shifts in the geo-political environment, the government of the United States has developed a new set of strategies to pursue its national security goals. These strategies identify current and projected capability gaps between the government's subordinate departments and the emerging threat environment and provide direction for change. Three of the guiding strategies for the United States military forces are *The National Security Strategy of the United States* (NSS), *The National Defense Strategy of the United States* (NDS), and *The National Military Strategy of the United States* (NMS).

[50] Ibid., 3-4.
[51] Ibid., 4-7.

The President's NSS directs an active strategy to counter transnational terrorist networks, rogue nations, and aggressive states that possess or are working to gain weapons of mass destruction or effect.[52] The NDS supports the NSS by "establishing a set of overarching defense objectives that guide the Department's security activities and provide direction for the National Military Strategy."[53] The purpose of the NMS is to provide "focus for military activities by defining a set of interrelated military objectives from which the Service Chiefs and combatant commanders identify desired capabilities and against which CJCS assesses risk."[54] The NMS captures the fundamental shift in the strategic environment in its opening paragraphs. It states, "**Adversaries** capable of threatening the United States, its allies, and its interests **range from states to nonstate organizations to individuals**… **Some of these adversaries are politically unconstrained and, particularly in the case of non-state actors, may be less susceptible to traditional means of deterrence.**"[55] (Emphasis added).

The NDS categorizes these threats and establishes a set of overarching defense objectives that guide the Department of Defense's security activities. These objectives serve as links between military activities and those of other government agencies in pursuit of national goals. In the NDS, the Department of Defense argues that because the U.S. military dominates the world in traditional forms of warfare, potential adversaries shift away from challenging the United States through traditional military action and adopt asymmetric capabilities and methods. The Department of Defense categorizes this array of challenges as traditional, irregular, catastrophic, and disruptive capabilities and methods that threaten U.S. interests. It defines each challenge as follows:

---

[52] Office of the President of the United States, *The National Security Strategy of the United States of America* (Washington: GPO, September 2002) 1, 5, 13.

[53] Headquarter, Department of Defense, *National Military Strategy of the United States of America* (Washington: GPO, 2004), 1.

[54] Ibid., viii.

[55] Ibid., 4-5.

> ***Traditional*** challenges are posed by states employing recognized military capabilities and forces in well-understood forms of military competition and conflict.
>
> ***Irregular*** challenges come from those employing "unconventional" methods to counter *traditional* advantages of stronger opponents.
>
> ***Catastrophic*** challenges involve the acquisition, possession, and use of WMD or methods producing WMD-like effects.
>
> ***Disruptive*** challenges may come from adversaries who develop and use breakthrough technologies to negate current U.S. advantages in key operational domains.[56] (Bold in original).

These categories overlap and recent experience indicates that the most dangerous circumstances arise when the United States faces a complex set of challenges. This monograph centers on the irregular threat, understanding that an irregular threat may employ catastrophic, disruptive, and traditional methods as well as irregular methods in its overall strategy. According to the NDS, the aim of adversaries using irregular methods is "to erode U.S. influence, patience, and political will."[57] It states, "Irregular opponents often take a long-term approach, attempting to impose prohibitive human, material, financial, and political costs on the United States to compel strategic retreat from a key region or course of action."[58] Irregular threats employing a strategy of prolonged conflict is a fundamental shift in the military aspect of the strategic environment. It signifies a shift from wars of annihilation to wars of attrition as the preferred strategy.

The Capabilities-Based Approach

Understanding future threats is a constant challenge in the transformation process. During the Cold War, the intelligence community estimated future threats based on evidence of capabilities and intentions from its major adversary, the Soviet Union. This evidentiary threat

---

[56] Headquarters, Department of Defense, *National Defense Strategy of the United States of America* (Washington: GPO, March 2005), 2.

[57] Ibid., 3.

[58] Ibid., 3.

provided a model that focused the Army's development of its systems and capabilities and shaped its doctrine and training. By having a detailed knowledge about its major adversary's requirements, and development and acquisition process, the Army could design systems that precisely targeted a known threat capability.[59] The Army institutionalized the spread of that knowledge to its officers and soldiers through its training and doctrine institutions. It produced a series of Soviet specific threat manuals that described the Soviets' operational and tactical preferences, their tables of organization and equipment, and the capabilities of their individual weapons platforms. The Army trained its brigades against a dedicated opposing force that replicated the expected actions of the Soviets and its surrogates at its Combat Maneuver Training Centers. That approach is no longer feasible for the emerging threat environment.

The fluidity of the new strategic environment has created a condition in which the threats are numerous, agile, and adaptive. There are traditional, evidentiary threats, but more numerous irregular threats are quickly overshadowing them. Unlike the traditional threats of the Cold War, the modern irregular threats quickly adapt to the changing pressures of their environments. One distinguishing characteristic of the emerging threat environment is the ability of irregular threats to gain access to military technologies and adapt readily available commercial technology to military purposes.[60] Another significant characteristic of the emerging threat is its use of complex forms of organizational structure, enabled by its use of the global information grid. Understanding the enemy now is less a matter of memorizing the rank and file of a specific armored column as it is conceptualizing the framework that promotes and sustains an irregular threat.

In order to develop a flexible force capable of countering the threats of the multi-polar world, the Department of Defense, and subsequently the Army, adopted a capabilities-based

[59] John F. Sandoz, *Red Teaming: Shaping the Transformation Process,* (Alexandria: Institute for Defense Analysis, 2001), 5, IDA, D-2590.

[60] Ibid., 5.

approach to force transformation. The 2001 QDR states that the capabilities-based approach reflects the fact that "the United States cannot know with confidence what nation, combination of nations, or non-state actor will pose threats to vital U.S. interests or those of U.S. allies and friends decades from now."[61] Its premise is that it is possible to anticipate the capabilities that an adversary might employ without knowing exactly which adversary will act. It focuses more on how an adversary might fight than who the adversary might be and where a war might occur.[62] The concept of the capabilities-based approach shapes the Department of Defense threat models and underpins its force transformation strategy.

The Joint Model: The Joint Operational Environment

The Department of Defense's emerging threat models address the threat in terms synonymous with the national strategies. These models provide better detail of the threat in the operational and tactical battlespaces. The joint forces threat model is contained in documents such as the white paper *Joint Operational Environment: Into the Future* (JOE). They concur that the operational environment will become more fluid as regional powers (in the form of states, coalitions, and alliances) and transnational actors emerge and fade from the international scene. According to the Joint Forces Command paper, threats will continue to challenge the United States on land, at sea, and in the air, but notes that urban terrain and complex terrain, such as mountainous regions, will dominate the land battlespace. It also notes that future threats, particularly transnational threats, will attempt to execute domestic strikes against the United States.[63]

---

[61] Headquarters, Department of Defense, *Quadrennial Defense Review Report* (Washington: GPO, September 2001), 13.

[62] Ibid., 13-14.

[63] Headquarters, Joint Forces Command, *The Joint Operational Environment: Into the Future,* Coordinating Draft, January 2005, 75-76.

The JOE identifies six operational design characteristics that current and future threats could center their operations on: 1) precluding U.S. involvement; 2) operationally excluding the United States from the region; 3) limiting U.S. access; 4) attacking the U.S. military system of systems; 5) setting conditions and conducting tactical and operational strikes; 6) and conducting pervasive strategic attack.[64] Taken in the context of a nation-state executing regional influence, none of these characteristics appears fundamentally different from characteristics of 20th century warfare. However, the concept that a non-state, transnational actor can design an operation with these characteristics and execute it against the United States is a significant shift in the operational environment from that of the Cold War.

Transnational, or non-state, actors leveraging the influence of 21st century information technology can organize people in movements commensurate with 20th century multi-national alliances. For example, religious networks and ideological networks can provide support to and sanctuary for transnational opponents. These networks provide several passive and active support mechanisms that elude U.S. counterstrikes. They provide a means to collect and disseminate information between dispersed elements by permitting transnational members to congregate in internationally recognized sanctuaries and by promoting nonviolent support actions such as physical and digital couriering of information. They provide moral justification for the transnational threat's actions and can actively work to gain the support of the local population. Networks of transnational organizations also provide front businesses that acquire dual use technologies, provide commercial transport, raise funds, and launder funds. Utilizing existing infrastructure, transnational threat organizations exploit multiple sources of power on par with states of the 20th century.

According to the JOE, the emerging threat is demonstrating an increased capability to shape the environment and shift its method of warfare to create asymmetric conditions that favor

[64] Ibid., 111.

its capabilities. The emerging threat will attempt to exploit the Army's reliance on systems warfare. It will design operations to deny sensor to shooter integration, deceive Intelligence, Surveillance, and Reconnaissance (ISR) collectors, and overwhelm the U.S. military intelligence system's analytical capability in order to deny the U.S. forces their technological advantages.[65]

A characteristic that is new to the emerging threat is its increased sophistication in information operations. The emerging threat has demonstrated significant capability to shape regional and local perceptions through local and global information systems. It has the capability to attack unsecured or poorly secured networks and it has the capability to purchase dual use technologies that deceive and defeat U.S. ISR capabilities. The future threat is an agile, technologically advanced and fiscally sound organization that operates across the depth of the global battlespace.[66]

The Army Model: The Contemporary Operational Environment

The Army presents an overview of its threat model in the *Army Strategic Planning Guidance* (ASPG). It adopts the four categories of security challenges put forth in the NDS and states, "These challenges are based on the recognition the old threat paradigm, focused primarily on other states and especially the military force-on-force capabilities of known enemies, is necessary but no longer sufficient after the attack on 9/11."[67] The United States will not deter the new threats emerging in the strategic environment with traditional military superiority. The ASPG proposes that irregular threats will present challenges that the United States may not be able to solve with traditional military solutions. It concedes, "The old concepts of security,

[65] Ibid., 114-115.
[66] Ibid., 117-119.
[67] Headquarters, Department of the Army, *Army Strategic Planning Guidance, Annex D: The Security Environment*, (Washington: GPO, 2005), 1. Accessed online at http://www.army.mil/references/ASPG-AnnexD.doc.

deterrence and warning, and traditional intelligence approaches to assessing threat capability, intent, and will, do not completely apply in this new strategic environment."[68]

The ASPG identifies terrorism as the most immediate danger from irregular threats. The gravest threat is from transnational terrorists such as Al Qaeda. It defines terrorism as "an asymmetric method used by irregular forces to force their will on others."[69] It also identifies that terrorism's root causes are complex, long-standing and not susceptible to short, purely military solutions. Because of this, it estimates that the GWOT will develop a characteristic similar to the Cold War or the War on Drugs: it will become persistent effort without a point of clear or decisive victory.

The ASPG projects that over time the military component of the GWOT may become less central and the war may require a coalition effort of intelligence and police actions.[70] It notes that Operation Iraqi Freedom illustrates many persistent threats and challenges in the future security environment. Military efforts there exemplify future military actions the Army expects: challenges not resolved by decisive combat, but fighting different factions of irregulars, criminals, and transnational terrorists.[71]

The ASPG projects a wide array of capabilities for the Army including the capability to conduct these lower intensity conflicts as well as the capability to conduct major combat operations against a regional power or coalition of adversaries. Although it commits to terrorism as the most dangerous potential adversary, it does not attempt to quantify or prioritize the capabilities its force needs. It concludes that the range of military options has never been larger

[68] Ibid., 2.
[69] Ibid., 5.
[70] Ibid., 5.
[71] Ibid., 6

and that the United States must be able to transition rapidly between missions or conduct simultaneous different missions with an appropriate mix of forces and capabilities.[72]

The Army refines its threat model for the capabilities-based approach in *FM 2-0, Intelligence.* It concurs with Department of Defense and national assessments that the operational environment is dynamic, multidimensional, and global. It highlights that this will require an increased flexibility in Army intelligence to both maintain regional knowledge of evidentiary threats, but also have the ability to gain threat-specific knowledge of emerging adversaries quickly. It also presents the premise that U.S. dominance in size, technology, organizational, and strategic capabilities is forcing opponents to adopt unconventional and adaptive tactics and operations to achieve their goals.[73]

The model in FM 2-0 consists of a framework that describes both the operational environment and the threat residing within it. It bounds the problem set of the COE using six dimensions of the operational environment and eleven critical threat variables. The six dimensions of the operational environment are threat, political, unified action, land combat operations, information, and technology. These six dimensions account for the increasing complexity of the multi-polar geo-political environment. Instead of focusing on only military aspects of the operational environment, FM 2-0 includes in the role of military intelligence an understanding of the political, ethnic, economic, and religious tensions that surround the military conflict. FM 2-0 recognizes the wide range of activities occurring within a unified command in the COE and stresses the importance of interoperability and integration between the joint intelligence structure and individual service intelligence systems. FM 2-0 contends that these

[72] Ibid., 7.

[73] Headquarters, Department of the Army, *FM 2-0: Intelligence* (Washington: GPO, May 2004), 1-19.

dimensions affect how the Army intelligence plans, prepares, executes, and assesses its missions.[74]

The eleven critical variables in FM 2-0 facilitate a commander's understanding of the threat. They are the nature and stability of the state, regional and global relationships, economics, demographics, information, the physical environment, technology, external organizations, national will, time, and military capabilities.[75] Woven throughout these subjects is an expectation that the commander's intelligence organization will provide him with region-specific knowledge of these variables and be able to provide an understanding of their interrelationships within the operational environment dimensions.

U.S. Threat Models

National	DoD	Army	
Four Challenges	**Six Operational Design Characteristics**	**Six Dimensions**	**11 Critical Variables**
Traditional Irregular Catastrophic Disruptive	Precluding U.S. involvement Operational exclusion Limiting access Attack US system of systems Tactical and operational strikes Pervasive strategic attack	Threat Political Unified action Land combat ops Information Technology	Nature and stability of the state Regional and global relationships Economics Demographics Information Physical environment Technology External organizations National will Time Military capabilities

Figure 2: Comparison of government threat models.

Adapted from concepts presented from *The National Defense Strategy of the United States of America* (Washington: 2004), *The Joint Operational Environment: Into the Future* (Joint Forces Command: 2005), and *FM 2-0, Intelligence* (Washington: 2004).

[74] Ibid., 1-20 to 1-23.
[75] Ibid., 1-23.

From national level to Army level, the threat models guiding the capabilities-based approach to force design consistently recognize the fundamental shift in the strategic geo-political environment from one of bi-polarity to one of multi-polarity. They concur that irregular threats are the most-likely emerging threat U.S. forces will face in land combat operations. Furthermore, they are consistent in considering an irregular force, probably a non-state actor, conducting a strategic attack with a weapon of mass destruction or effect as the most-dangerous scenario threatening U.S. security. This transnational capability to create mass casualties is a significant shift from the United States' experience in the 20th century. The Army model centers on understanding the political, cultural, social, religious, and military characteristics specific to a named threat in order to provide predictive, intent based, intelligence. These same characteristics are present in the evidentiary threat of Al Qaeda.

CHAPTER FIVE

GLOBAL INSURGENCY, A NEW FORM OF WAR?

Irregular forces were not unheard of during the Cold War. The United States and its NATO partners conducted military operations against insurgents and terrorist organizations and developed policies, doctrine, and tactics to address these threats throughout the 20th century. Modern insurgencies, or insurgencies of the last half of the 20th century, are most similar to the emerging irregular threat because of their access to modern technology and their use of terror as a tactic. As an evidentiary threat, they provide a basis of comparison for analysis of the emergent threat. In order to understand specific capabilities of an evidentiary threat, this study focuses on published analysis of Al Qaeda, a transnational, irregular threat that the State Department has identified as a Foreign Terrorist Organization.[76]

Terrorists, insurgents, and irregular forces

It is important to distinguish between insurgency, irregular forces, and terrorists to define the emerging threat. The Department of Defense defines an insurgency as "an organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict."[77] It defines irregular forces as "armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces."[78] The Department of Defense defines terrorism as "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."[79] Terrorism is a tactic. A

[76] US Department of State, Office of the Coordinator for Counterterrorism, *Country Reports on Terrorism 2004.* (Washington: Department of State Multimedia Services, April 2005), 92. Department of State Publication 11248.

[77] Headquarters, Department of the Army, *FM 1-02: Operational Terms and Graphics*, (Washington: GPO, September 2004), 1-101.

[78] Ibid., 1-105.

[79] Ibid., 1-187.

traditional military force, police force, an insurgency, or a transnational actor could employ the tactic of terrorism. When a group that is not part of a state apparatus employs the tactic of terrorism it is a terrorist group; the individuals of the group are thereby terrorists. The Department of Defense defines a terrorist as "an individual who uses violence, terror, and intimidation to achieve a result."[80]

To focus the research of this paper, the author recognizes three categories of terrorist groups: domestic, international, and transnational. A terrorist group that operates within the confines of a single nation is a domestic terrorist group. A terrorist group that resides in one region or state or receives sponsorship from a state, but acts across national boundaries to attack either its opponents or those of its sponsor is an international terrorist group. The most recent category of terrorist group attacks across multiple states, similar to the international terrorist, but does not have a state sponsor. Therefore, non-state actors who employ the tactic of terrorism are transnational terrorist groups.[81]

An insurgency is the most likely manifestation of the emerging irregular threat. The ASPG states, "Irregular forces could arise in any insurgency or operation where the Joint Force might be called upon to act. Among irregular forces, the gravest threat is from global transnational terrorists, especially from radical Sunni extremists like Al Qaeda."[82] One critical difference between insurgencies of the latter 20th century and the emerging transnational irregular threat is scope. The previous insurgencies operated against a single constituted government. The

---

[80] Ibid., 1-187.

[81] Bard E O'Neill, *Insurgency & Terrorism: From Revolution to Apocalypse* (Washington, DC: Potomac Books, Inc.), 34. Bard O'Neill identifies these three categories and recognizes that they are not universally accepted. Joint and Army doctrine surveyed for this research did not distinguish between terrorist groups in this manner. The distinction is critical to understanding the framework of the threat, especially at the tactical level. A division's area of interest encompasses the threat's support base. Depending on the category of terrorist group a division faces, its area of interest could range from a specific district within a state to the entire planet. This greatly affects the capabilities the division G2 must have in order to understand and collect against a transnational terrorist organization.

[82] Headquarter, Department of the Army, *Army Strategic Planning Guidance, Appendix D: The Security Environment*, (Washington: GPO, 2005), accessed online at http://www.army.mil/references/ASPG-AnnexD.doc, 2.

emerging threat has a broader regional focus. If a transnational terrorist group is an organized movement that aims to overthrow constituted governments, then it presents a new form of warfare. That form of warfare is regional, and possibly global, insurgency, or pansurgency. A pansurgency is "an organized movement of non-state actors aimed at the overthrow of values, cultures, or societies on a global level through the use of subversion and armed conflict, with the ultimate goal of establishing a new world order."[83]

Al Qaeda, the insurgency

Bard O'Neill, a professor at the National War College in Washington, D.C. with over 40 years of experience in researching insurgencies, provides a framework for studying an insurgency in his book *Insurgency & Terrorism: From Revolution to Apocalypse*. This framework provides a conceptual context from which one can deduce similarities and differences between the characteristics of the emerging irregular threat and evidentiary irregular threats as well as identify changes within a specific insurgency. O'Neill's concept considers three factors: the existing political situation, from which the insurgents define their goals or desired changes, the insurgency itself, and the government's response to the insurgency. His framework of the insurgency consists of five variables: the nature of the insurgency, the environment, popular support, organization and unity, and external support. He includes a sixth variable that describes the government's response to the insurgency. Within each of these, he further categories the characteristics of common types of insurgencies. O'Neill did not design the framework to provide a perfect fit between these characteristics and a specific insurgency, but to provide a set

[83] Jay Chambers and others, *Combating Terrorism in a Globalized World: Report by the National War College Student Task Force on Combating Terrorism,* (Washington, DC: National Defense University, 2002), 10. Document available online from: http://www.au.af.mil/au/awc/awcgate/ndu/n02combating_terrorism.pdf.

of descriptors that help an analyst bound his study.[84] Figure three provides a summary of his framework.

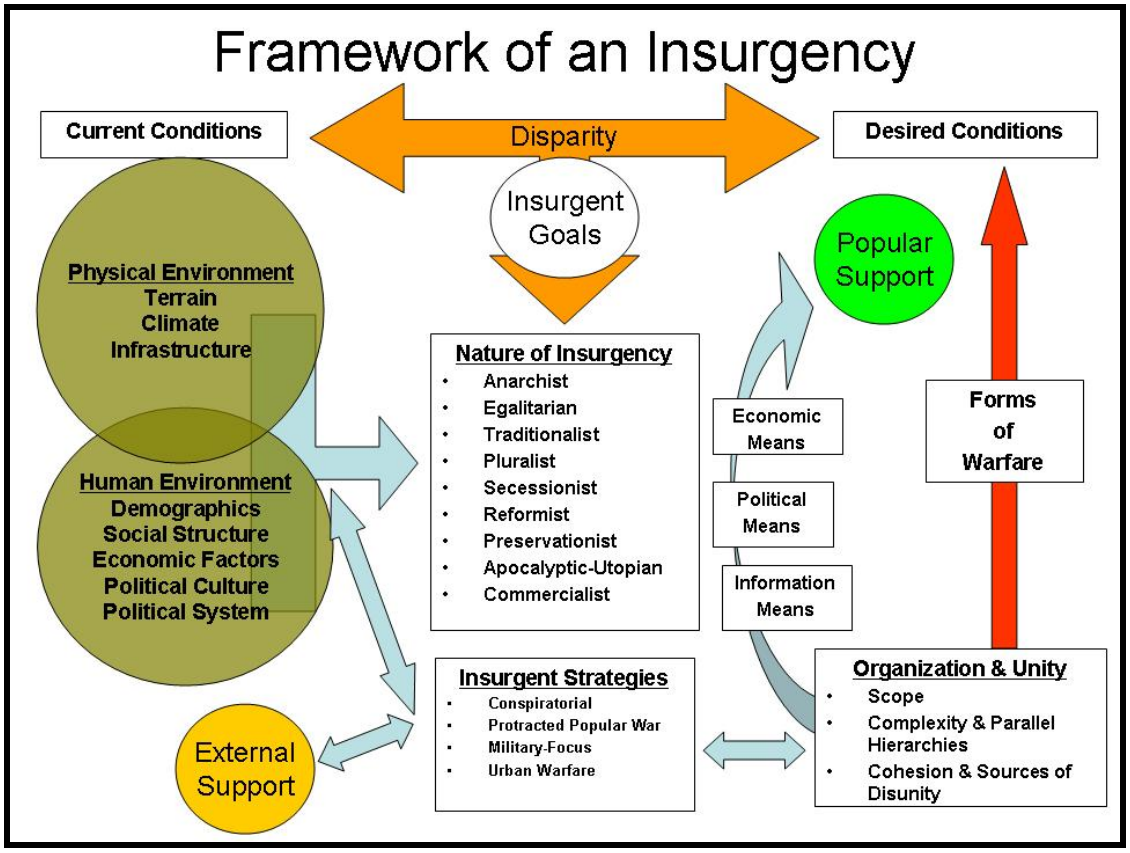

Figure 3: O'Neill's framework for an insurgency.

Adapted from Bard E. O'Neill, *Insurgency & Terrorism: From Revolution to Apocalypse* (Washington, D.C.: Potomac Books, Inc., 2005).

Al Qaeda presents a fundamental shift from that of terrorist organizations and insurgents of the 20th century. Their operational capability to conduct transoceanic strategic attacks and sophisticated ambushes using a complex global infrastructure indicates that they are an insurgency on an order of magnitude never before witnessed. It is clear using O'Neill's framework that the irregular threat Al Qaeda presents is a dynamic, adaptive threat that is

[84] O'Neill, 11-13 and 201-202.

significantly different from previous irregular threats. They are at least a regional insurgency if not the first global insurgency.

Prior to U.S. Operation ENDURING FREEDOM in Afghanistan Al Qaeda held characteristics typical of most 20th century irregular threats. O'Neill categorizes Al Qaeda as a networked organization most similar to the traditionalist insurgency that uses the military focus strategy to achieve its goal.[85] In articulating their goals of re-establishing the caliphate and uniting all Muslim people under one Salafist state, Al Qaeda demonstrated the characteristic of a traditionalist insurgency. Insurgencies that demonstrate the traditionalist nature speak of sacred values and found their cause in religion or ancestral ties. They often seek to restore a political system and may idealize a former era as a "golden age." These O'Neill subtypes as *reactionary-traditionalists*. Al Qaeda theoretician Faris Al Shuwayl al-Zaharani expressed Al Qaeda's goal as, "The rulers of the countries of Islam in this age are all apostate, unbelieving tyrants who have departed in every way from Islam. Muslims who proclaim God's unity have no other choice than iron and fire, jihad in the way of God, to restore the caliphate according to the Prophet's teachings."[86]

As O'Neill notes, one of the challenges of identifying the nature of an insurgency is identifying its goals that may change over time. Additionally, differentiating between intermediate and ultimate goals can cause confusion in determining the type of the insurgency. Al Qaeda's founders argued on the best approach to achieve its goal. Some sought the overthrow of an apostate regime while others, principally Osama bin Laden, sought the eviction of Western powers from the Arabian Peninsula. On 23 February 1998, Al Qaeda created the World Islamic Front for Jihad Against the Jews and Crusaders and issued a declaration in which Osama bin

[85] Ibid., 21-22, 56-60, 65-66, 120, and 132. O'Neill addresses each characteristic of Al Qaeda by chapter in this latest edition of his work. The above statement summarizes the basic elements of his categorization.

[86] Ibid., 22. O'Neill sources the quote from *Al Hijaz* (London), August 15, 2004, in *FBIS-Near East South Asia*, August 15, 2004.

Laden stated, "The ruling to kill the Americans and their allies, civilians, and military, is an individual duty for every Muslim who can do it in any country in which it is possible to do it, in order to liberate the al-Aqsa mosque and the holy mosque from their grip, and in order for their armies to move out of all the lands of Islam."[87]

This statement indicated a shift in Al Qaeda's intermediate goals from the "near enemy," or local regimes it considered apostates to the "far enemy," or the United States. It also indicated a shift in the nature of the insurgency. Al Qaeda shifted from supporting individual insurgencies within the confines of different Middle East nations to establishing an insurgency that seeks to establish a worldwide political system. It seeks to replace multiple national political systems with a single political system.

Al Qaeda uses the means of information operations, social action, political action, guerrilla warfare and terrorism. However, it subordinates political action to military action to achieve political effects. It relies heavily on irregular warfare tactics and information operations to gain asymmetric advantages against its adversaries. It also exploits the asymmetric benefits of urban terrain and complex rural terrain depending on the environment of the specific region of conflict across its global battlespace.

Al Qaeda has trained and employed both conventional and unconventional fighters. Prior to Operation ENDURING FREEDOM, Al Qaeda developed a guerrilla organization it called the 055 Brigade. The 055 Brigade consisted of about 2,000 guerrillas that served as Al Qaeda's strategic reserve. From 1997 to 2001, it integrated with the Army of the Islamic Emirate of Afghanistan and fought the Northern Alliance employing conventional Soviet weapons in a combination of conventional and irregular tactics. After suffering significant losses in 2001, the remnants of the 055 Brigade retreated into the complex terrain of the Afghanistan-Pakistan border

[87] Rohan Gunaratna, *Inside Al Qaeda* (New York: Columbia University Press, 2002; Berkley Books, 2003), 61.

region to conduct a protracted campaign.[88] In addition to the 055 Brigade, disparate published reports indicate that Al Qaeda trained between 10,000 and 110,000 fighters in Afghanistan between 1989 and 2001 who have since dispersed to an approximately 60 countries. This provides them with a force pool larger than 61 of the world's 161 armies. Al Qaeda is quite selective in its recruitment, though, historically accepting only about three percent of those fighters trained into its official ranks. [89]

Al Qaeda strategically employs diplomatic, informational, and economic sources of power. It has developed symbiotic coalitions and alliances with other insurgent organizations and some states. Al Qaeda's cooperation with the Taliban government in Afghanistan is only one example of its cooperation with state actors. Al Qaeda has a history of developing front businesses, exploiting Non-Governmental Organization (NGO) access, developing commercial ventures, bribing government officials, and providing basic social services.[90] Al Qaeda established a robust training and financial infrastructure in addition to its bases in Afghanistan Pakistan, and Sudan. While in Sudan, Osama bin Laden developed businesses to serve as front companies for his network and as legitimate businesses to produce income for the organization. He also negotiated agreements with the president of Sudan, Brigadier Omar Hassan Ahmad al-Beshir. Among other guarantees, Beshir provided protection to Wadi al-Aqiq, one of Osama bin Laden's firms, which enabled Al Qaeda to import goods without inspection or payment of taxes. Bin Laden also developed relationships with Sudan's political, intelligence, and military organizations. His relationships and investments not only guaranteed state support for Al Qaeda

[88] Ibid., 80-81.

[89] Michael F. Morris, "Al Qaeda as Insurgency," Joint Forces Quarterly #39 (Washington, DC: Institute for National Strategic Studies, October 2005), 43. Available online at http://www.dtic.mil/doctrine/jel/jfq_pubs/issue39.htm and Rohan Gunaratna, *Inside Al Qaeda* (New York: Columbia University Press, 2002; Berkley Books, 2003), 11.

[90] O'Neill, 65-66.

but also provided Sudan with support that included intelligence information from his network and significant financial inflows.[91]

Al Qaeda's information operations include the publication of books and pamphlets, exploitation of the internet, and broad access to the Arab media. It projects messages focused on both the near and far audience. It influences the near audience through the declaration of *fatwas* and publication of audio and video messages through the internet and global media. It influences the far audience, western governments and will of their peoples, through violent action in concert with specific messages. It explicitly synchronizes its military actions and its information operations to achieve a specific political effect. O'Neill notes, "The purpose of the Madrid bombing in March 2004 was to influence the national elections so that a new government would be installed that would withdraw Spanish troops from Iraq."[92]

Al Qaeda's demonstrated capability to wield diplomatic, informational, and economic sources of power as well as a military source of power underpin its ability to lead the Global Salafi Jihad. Sageman describes the Global Salafi Jihad as "a worldwide religious revivalist movement with the goal of reestablishing past Muslim glory in a great Islamist state stretching from Morocco to the Philippines, eliminating present national boundaries."[93] It is not a specific organization, but a social movement that Sageman describes as "consisting of a set of more or less formal organizations, linked in patterns of interaction ranging from the fairly centralized to the more decentralized and with various degrees of cooperation."[94] Al Qaeda serves as the vanguard of this social movement.

Title 22 of the US Code, Section 2656f, requires the Department of State to provide an annual report to Congress on terrorism. It requires the report to include information on terrorist

---

[91] Gunaratna, 40-42.
[92] O'Neill, 34, 65.
[93] Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004), 1.
[94] Ibid., 137.

groups and umbrella groups under which any terrorist group falls. The 2004 *Country Reports on Terrorism* lists 40 Foreign Terrorist Organizations and identifies twelve of those as associated with or linked to Al Qaeda. It also lists 40 Other Selected Terrorist Organizations, of which nine are associated with or linked to Al Qaeda.[95] Clearly, with known ties to over one quarter of the world's terrorist organizations deemed a threat to U.S. security, Al Qaeda is taking a leading role in the Global Salafi Jihad.

Al Qaeda, the organization

To serve as the vanguard of this movement, Al Qaeda has created a global cellular organization that emphasizes social connections. It focuses on supporting and conducting military operations rather than developing a parallel hierarchy to replace the government of deposed regimes.[96] As a complex adaptive system, Al Qaeda adapted to changes in its environment with changes to its organizational structure. It continues to change as the United States and coalition partners continue to attack it. Prior to Operation ENDURING FREEDOM, Al Qaeda operated largely in an overt manner, but as attacks threatened its existence, it has transformed into a more clandestine organization.

Al Qaeda is essentially a networked organization, but it also contains functional organizations within the network and employs matrix organizations to conduct specific activities. It uses this organizational structure to conduct netwar operations. Netwar is a concept put forward by RAND authors John Arquilla, David Ronfeldt, and Michele Zanini, in their 1999 article "Networks, Netwar, and Information Age Terrorism." They define netwar as:

> an emerging mode of conflict and crime at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the

[95] US Department of State, Office of the Coordinator for Counterterrorism, *Country Reports on Terrorism 2004.* (Washington: Department of State Multimedia Services, April 2005), 92, 113. Department of State Publication 11248.

[96] O'Neill, 190.

information age. These protagonists are likely to consist of dispersed small groups who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command. Thus, information-age netwar differs from modes of conflict and crime in which the protagonists prefer formal, standalone, hierarchical organizations, doctrines, and strategies, as in past efforts, for example, to build centralized movements along Marxist lines.[97]

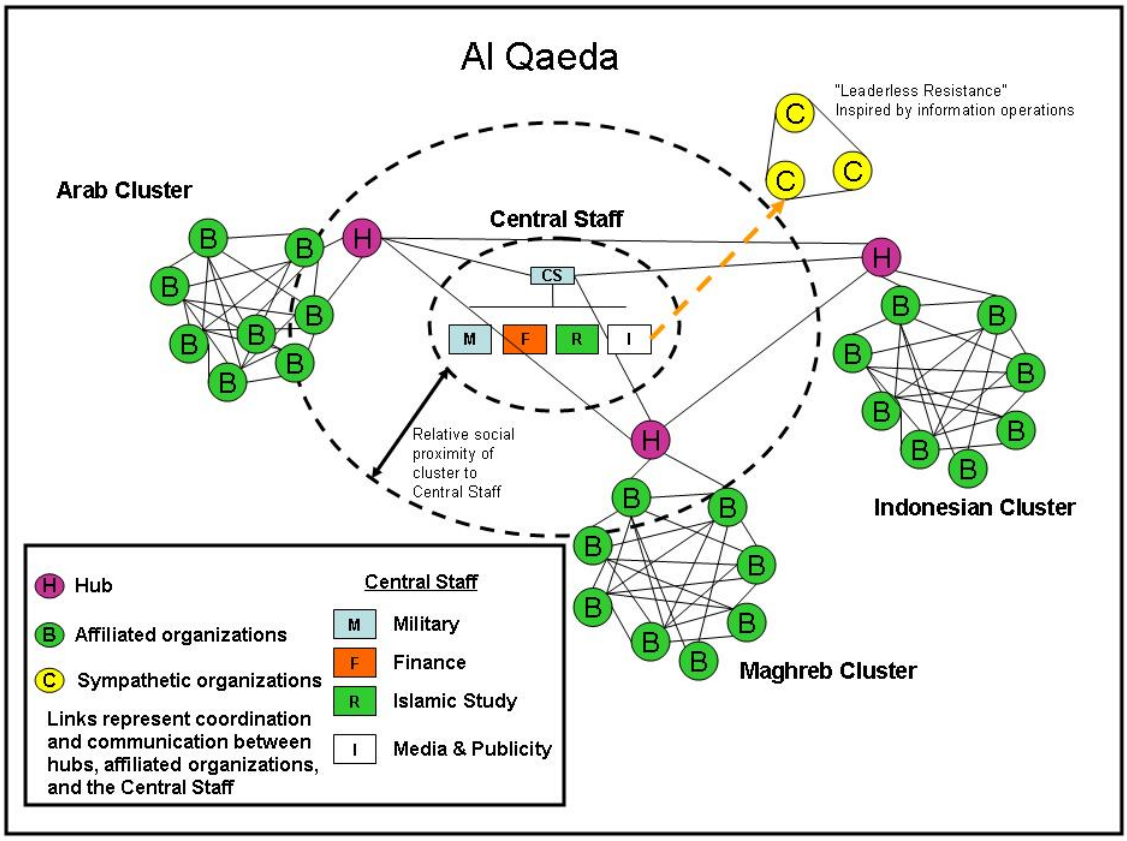

Figure 4. A conceptual model of Al Qaeda.

This concept merges topics from Sageman, Gunaratna, O'Neill, and Garfinkel. The Central Staff maintains a functional structure and supports clusters of organizations throughout the world with operational guidance, financing, and resources. Information operations from the Central Staff inspire sympathetic persons and organizations who then take unilateral action.

[97] John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information-Age Terrorism," in Ian O. Lesser et al., Countering the New Terrorism (Santa Monica, Calif.: The RAND Corporation, MR-989-AF, 1999), p. 47.

Al Qaeda's network consists of two echelons or concentric groupings: an inner core and an outer core. The inner core is the central structure that consists of the founding leaders of the organization and four functional committees: military, finance and business, *fatwa* and Islamic study, and media and publicity. Almost two-thirds of its members are Egyptian. It plans and directs guerrilla and terrorist attacks of its own, normally focused on strategic targets, but has not been directly involved in conducting operations since 1996. It primarily coordinates with, inspires, and instigates attacks by the affiliated groups. The lead person for the central structure, who is also the central figure of the organization, is Osama bin Laden.[98]

Immediately outside this innermost circle are three groupings of terrorists, or clusters: the Core Arab cluster, the Maghreb Arab cluster and the Southeast Asian cluster. Each cluster consists of a set of terrorist organizations and individuals. Each cluster has at least one identifiable key figure or hub that provides a linkage between the clusters and the central structure. Although all three clusters have been involved in regional attacks, the Core Arab cluster has been responsible for the attacks of greatest strategic importance, such as the attacks of 11 September 2001. It consists of terrorists from the core Arab states. A Saudi Arabian majority dominates it with other major contributors coming from Egypt, Yemen, and Kuwait.[99] The Maghreb Arab cluster comes primarily from France, Algeria, Morocco, and Tunisia. It consists of second-generation French citizens of Maghreb descent and some converts to Islam. They have been involved in the millennial plots against targets in Amman and Los Angeles, the plot to attack the US embassy in Paris, and the Richard Reid shoe bomber plot.[100] Indonesians dominate the Southeast Asian cluster and it is closely associated with the terrorist organization Jemaah Islamiya. It is more hierarchical than the other two clusters. An amir and his consultative council lead Jemaah Islamiya. It consists of four regions with each region further divided into branches.

[98] Sageman, 42-43, 70-72, 137-138.
[99] Ibid., 46, 48, 70, 137, 141.
[100] Ibid., 46, 48, 72, 137, 141.

The head of each branch serves as a consultative council to which staff units report. One of these units is an operations unit that consists of operational cells of four to five people.[101]

The organizational structures of the individual groups that make up the three clusters in the outer core vary, as do their relationships with Al Qaeda. Some organizations simply cooperate with Al Qaeda, such as Lashkar e-Tayyiba the armed wing of the Pakistan-based religious organization, Markaz-ud-Dawa-wal-Irshad (MDI), an anti-U.S. Sunni missionary organization formed in 1989. It provided sanctuary for senior Al Qaeda lieutenant Abu Zubaydah. Coalition forces captured Zubaydah at one of these safe houses in Faisalabad in March 2002.[102] Other organizations have formally affiliated themselves with Al Qaeda, and Al Qaeda has absorbed, or annexed, others. In 2001, Al Qaeda annexed the Egyptian Islamic Jihad and in 2004, Jordanian Palestinian Abu Mus'ab al Zarqawi merged his organization, Tanzim Qa'idat al-Jihad fi Bilad al Rafidayn (QJBR, or Al Qaeda of Jihad Organization in the Land of the Two Rivers) with Osama bin Laden's Al Qaeda.[103]

Since the initiation of U.S. retaliatory action, Al Qaeda has suffered significant losses to its leadership and may have lost much of its ability to coordinate operations between the clusters leading some to speculate on shifts in the organization's structure and strategy. Sageman notes that the organization is resilient to attacks on its periphery, but fragile when attacked against its hubs. Recent attacks have left each of the clusters without key hubs or leaders that may degrade the organization's near-term ability to coordinate operations.[104] Furthermore, attacks on the network may cause it to assume a more decentralized network for tactical survival. By decentralizing, it can insulate clusters and subordinate organizations by providing support from

[101] Ibid., 46, 49, 70, 72, 138, 141.

[102] US Department of State, Office of the Coordinator for Counterterrorism, *Country Reports on Terrorism 2004.* (Washington: Department of State Multimedia Services, April 2005), 103. Department of State Publication 11248.

[103] Ibid., 101, 111.

[104] Sageman, 141.

multiple local sanctuaries; however, such a tactic could result in strategic failure. The organization may not be able to control the network and continue directing it toward the stated goal of establishing the caliphate.

Continued pressure on the network could result in transforming the organization of Al Qaeda into a movement of leaderless resistance. Leaderless resistance is a strategy popularized by anti-government activist Louis Beam in the 1980s and 1990s in which small groups and individuals fight an established power through independent acts of violence. In the United States, certain animal rights and environmental organizations, as well as Beam's anti-government associates, have used leaderless resistance. It allows an organization to exploit the freedoms of liberal democracy to establish sanctuary and promote its ideology. Leaderless resistance is a phenomenon closer to an ideological movement than an organized resistance. It consists of two elements, a non-violent ideologue who exploits the global information network and semi-independent cells that conduct acts of violence. The cells are leaderless because they do not have any central coordination and they do not have explicit communications with one another. A cell member may be inspired only by information publicized through the global information network and only act once in his life. Because of the extreme decentralized organization of leaderless resistance, it is resistant to infiltration and difficult to deconstruct with analytical tools such as link analysis. It provides protection to the leaders and ideologues by preventing formal linkages between the non-violent (and largely legal) motivational action, or information operations, and the violent actions carried out by the cells.[105] As a leaderless resistance, the Global Salafi Jihad could exist just below the surface like a smoldering forest fire, unable to flare up and achieve its strategic goal, but insulated from decisive military action.

[105] Simson L. Garfinkel, "Leaderless Resistance Today," accessed online from http://www.firstmonday.org/issues/issue8_3/garfinkel and Jessica Stern, "The Protean Enemy (al Queda)," in *Foreign Affairs*, 01 July 2003, accessed online from http://www.ksg.harvard.edu/news/opeds/2003/stern_protean_enemy_foraffairs_070103.htm.

The threat has changed in the contemporary operating environment. The evidentiary threat of Al Qaeda demonstrates characteristics that are consistent with the Department of Defense threat models. It is an agile adversary; it has adapted its organizational structure and its operations to the variations in the dimensions of its operating environments. It is a technologically advanced organization, which it demonstrates through its militarization of commercial technologies. It is a fiscally sound organization; it has proven its ability to produce the income it needs to sustain its operations without state sponsorship.

Al Qaeda operates across the depth of the global battlespace. It has the capability to conduct kinetic and non-kinetic operations and seeks victory through attrition rather than decisive battle. Al Qaeda is the manifestation of the threat models' most-likely adversary, a transnational irregular threat. It has demonstrated in word and deeds the desire to attack the United States with a weapon of mass destruction or effects; therefore, it is possible Al Qaeda may execute the threat models' most-dangerous course of action, a strategic attack against an American target to elicit mass casualties. Its characteristics are fundamentally different from the characteristics of the Soviet army and the revolutionary armies it supported, but consistent with the characteristics of the threat models for the contemporary operational environment. Therefore, Al Qaeda's characteristics provide a good baseline for the Army's intelligence capability to counter an irregular threat. It does not ignore the capability requirements the Army will also need to face the other security challenges outlined in the National Defense Strategy, but discounts their priority because the immediacy of the evidentiary threat places a current demand on the scarce intelligence resources.

CHAPTER SIX

CONCLUSIONS ON THE THREAT & RECOMMENDATIONS FOR INTELLIGENCE TRANSFORMATION

This chapter concludes the analysis of the evidentiary and emerging threats and compares the characteristics of the threat to the characteristics of the emerging modular intelligence system. It focuses on the development of the modular division's intelligence architecture. It assesses, through the lens of organization theory, the effectiveness of a modular division's intelligence capability to collect against a transnational insurgency and provide predictive intelligence products to supported commanders. Many of the concepts in the intelligence capability, such as the Battlefield Surveillance Brigade, are still emerging and not approved for fielding. Additionally, the compositions of the intelligence capability for the various brigades (light, heavy, STRYKER) differ by unit type. Therefore, a detailed discussion of the individual makeup of a specific unit would be argumentative at best. However, analysis of the characteristics of the threat lead to deductions of capabilities the Army intelligence system needs to counter them. These deductions demonstrate the value of various organizational structures, command relationships, and systems capabilities.

What capabilities do the threat's characteristics require?

Al Qaeda operates across the depth of the global operational environment. Therefore, the modular division must be able to operate across the global operational environment. However, Al Qaeda has adapted its organizational structure and its operations to the variations in the critical dimensions of its operating environments. Therefore, the Army intelligence capability must include the ability to understand the variations in the identified critical dimensions of the operational environment and provide that regional knowledge to a globally deployable modular division.

Al Qaeda demonstrates its technological prowess through its militarization of commercial technologies. The modular division must have the capability to exploit these same technologies. Regardless of the adversary's means of coordination, the modular division must be able to exploit the messages transmitted. Therefore, the modular division must not only have a generic SIGINT and HUMINT capability, but it must have the capability to receive functional organizations that specialize in exploiting various modes of communication and specialize in regional languages and dialects.

Al Qaeda is a fiscally sound organization; it has proven its ability to produce the income it needs to sustain its operations without state sponsorship. The logistics of this war centers on commercial banking and civilian enterprise. The modular division must have the ability to understand this type of logistical infrastructure by accessing experts in business, commerce, and finance. It must be able to exploit the lines of communication used by the emerging threat by understanding commercial traffic networks.

Al Qaeda has the capability to conduct kinetic and non-kinetic operations and seeks victory through attrition rather than decisive battle. To counter this, the modular division needs the capability to understand not only the threat's military source of power, but also its diplomatic, informational, and economic sources of power. The intelligence capability of a modular division must be able to know the structure and capabilities of the threats non-kinetic organizations and understand the interrelationships between kinetic operations and ensuing information operations.

Is intelligence transformation on track?

In September 2003, Secretary of Defense Donald Rumsfeld identified optimizing intelligence capabilities as one of his top ten priorities. Consequently, the Department of the Army established Task Force Modularity to develop the capability requirements of the modular units and Task Force Actionable Intelligence to develop the Army intelligence capability to support the new modular force. Using a capabilities-based approach, these organizations

recommended fundamentally changing the way the Army thinks about and performs intelligence collection, analysis, production, and dissemination.

Task Force Actionable Intelligence pursued four overarching concepts to change how the Army conceptualized intelligence support. These four concepts were changing the culture and mindset of intelligence producers and consumers, enhancing battlespace intelligence capabilities, implementing overwatch, and establishing a network enabled environment.[106] The most fundamental change within Army intelligence transformation is an effort to change the behavior and expectations of intelligence producers and consumers. The Army leadership views this as an essential step toward changing organizational and operational culture. Intelligence producers will transition from a current requirements orientation to an anticipatory approach while consumers shift their mindset from one of fighting with knowledge to one of fighting for knowledge. This new mindset views every soldier as a collector and as an analyst. Its initiatives include organizational, procedural, and technological changes that facilitate anticipatory intelligence and incorporate reports and insights from all echelons.[107]

One of the greatest challenges Army intelligence has faced is the ability to support the maneuver commander throughout his operation, from pre-deployment through re-deployment, with continuous integrated intelligence support. The tension between the transformation design requirement of globally oriented modular forces and the commander's need to understand a specific threat and region once deployed exacerbate this problem. The Army intelligence leadership plans to mitigate this tension by applying a mix of generalist and specialist organizations across its intelligence echelons and provide initiatives to address regional requirements.

---

[106] Headquarters, Department of the Army, *United States Army 2004 Transformation Roadmap* (Washington: Army Transformation Office, July 2004), 5-16.

[107] Ibid., 5-16 and Joe Burlas, "Initiatives Seek to Transform Army Intelligence Capabilities," *Army News Service* 13 April 2004, accessed online from http://www4.army.mil/ocpa/print.php?story_id_key=5848.

Many of the Army intelligence transformation initiatives seek advancements in the fields of data processing, analysis and fusion. As the *United States Army 2004 Transformation Roadmap* states, "The objective is to reach a point where the commander receives relevant data that is presented in an intuitive manner."[108] The Army faces significant challenges in separating relevant information from background clutter and fusing data from multiple, sources to deduce a coherent and consistent picture of the battlespace. For example, one of the ongoing and programmed initiatives listed in the Army Transformation Roadmap is the Information Dominance Center (IDC). The former deputy director of Task Force Actionable Intelligence described the IDC as "a state-of-the-art operational intelligence organization" that had "pioneered processes and methodologies for rapid fusion and analysis of complex threat networks and activities."[109] Conflicts between its ability to gather information, the legislative separation between domestic and foreign intelligence activities, interagency competition, and academic speculation brought the IDC to the news forefront in December 2005. The IDC reportedly successfully data mined a significant amount of information about Al Qaeda in 2000, but was forced to destroy it because, among other factors, its automated data mining capability risked collection against U.S. citizens, a legal prohibition.[110]

Tactical overwatch is another initiative that attempts to address the need for regional specialization. It is a combination of procedures, networked communications, and analytical capabilities that focus higher-echelon intelligence in direct support of tactical units. The tactical overwatch capability resides within five regionally focused Theater Intelligence Brigades (TIBs).

---

[108] Headquarters, Department of the Army, *United States Army 2004 Transformation Roadmap* (Washington: Army Transformation Office, July 2004), 5-16.

[109] Stephen K. Iwicki, "CSA's Focus Area 16: Actionable Intelligence: National, Joint, and Expeditionary Capabilities," *Military Intelligence Professional Bulletin* (July-September 2004), Accessed online from http://www.findarticles.com/p/articles/mi_m0IBS/is_3_30/ai_n13821812/print.

[110] Shane Harris, "Army Project Illustrates Promise, Shortcomings of Data mining," *National Journal*, accessed online from Govexec.com homepage at http://www.govexec.com/dailyfed/1205/120705nj1.htm.

Tactical overwatch provides region specific intelligence to a maneuver commander by concentrating a set of resources from the TIB directly on a subordinate division's area of responsibility. It provides continuous coverage while the modular division prepares for deployment, conducts movement, and commences operations. Conversely, once the division has deployed its collectors, it will compliment the theater capability by providing focused collection and analysis back to the TIB.[111]

The Army intelligence system must be fully integrated and interoperable in order to provide the focused, region-specific knowledge commanders require. The Army plans to develop a network-enabled environment to provide the integration and fusion framework that will link actionable intelligence to the supported war fighter. In the near term, Army efforts are concentrated on improving the quality and quantity of sensors, reporting means and analysis. Its initial focus has been on the Brigade Combat Team. The Army has accelerated integrating future capabilities into the current force by, for example, fielding an interim Distributed Common Ground System-Army (DCGS-A) and fielding organic military intelligence companies in the modular Brigade Combat Teams.

The Modular Division

To improve battlespace intelligence capabilities, task force modularity recommended several organizational changes to the traditional tactical military intelligence architecture for the modular division structure. FM 2-0, *Intelligence* states, "The Intelligence BOS architecture provides specific intelligence and communications structures at each echelon from the national level through the tactical level. These structures include intelligence organizations, systems, and procedures for collecting, processing, analyzing, and delivering intelligence and other critical

[111] Headquarters, Department of the Army, *United States Army 2004 Transformation Roadmap* (Washington: Army Transformation Office, July 2004), 5-16 and *Army Intelligence Comprehensive Guide to Modularity*, 11 May 2005, 16.

information in a useable form to those who need it, when they need it. Effective communications connectivity and automation are essential components of this architecture."[112]

The changes in organizational structure in the modular brigade and division will redefine the procedures for collecting, processing, analyzing, and delivering intelligence. The first dramatic change in the modularity concept is the development of a robust collection and analysis capability in the Brigade Combat Team (BCT). This capability includes the creation of a ground reconnaissance element, a significantly larger intelligence staff section, and the establishment of a military intelligence company organic to the Brigade Combat Team (BCT). This change reformed the CEWI battalion concept. It is providing dedicated capabilities to the maneuver brigades and is modernizing their systems' capabilities to provide collection and analysis tools designed against demonstrated evidentiary threat capabilities. These assets are now organic to brigade maneuver forces, greatly enhancing the maneuver commander's ability to develop an understanding of his tactical environment. The Army contends that these efforts will establish the right mix and balance of capabilities between the BCT, modular division, and theater and provide complementary and reinforcing coverage and to ensure continuity.

Unresolved issues concerning this initiative include training oversight of the intelligence soldiers, readiness oversight of their systems, and balancing generalist and specialist skills. The military intelligence company organic the maneuver brigade has a wide array of specialties and little internal capability to train and maintain them. Without a divisional intelligence battalion, the BCTs intelligence company commander lacks the resources it provided such as consolidated language training programs and consolidated maintenance facilities for their technical collection equipment. As globally oriented BCTs, the intelligence specialists will not focus their efforts on developing an expertise on any one region. Regional expertise will reside above the division in

[112] Headquarters, Department of the Army, *FM 2-0: Intelligence.* (Washington D.C: 17 May 2004), 1-3.

the TIBs and other strategic intelligence organizations. Again, balancing generalist and specialist capabilities are in tension as they were prior to the establishment of the CEWI battalion.

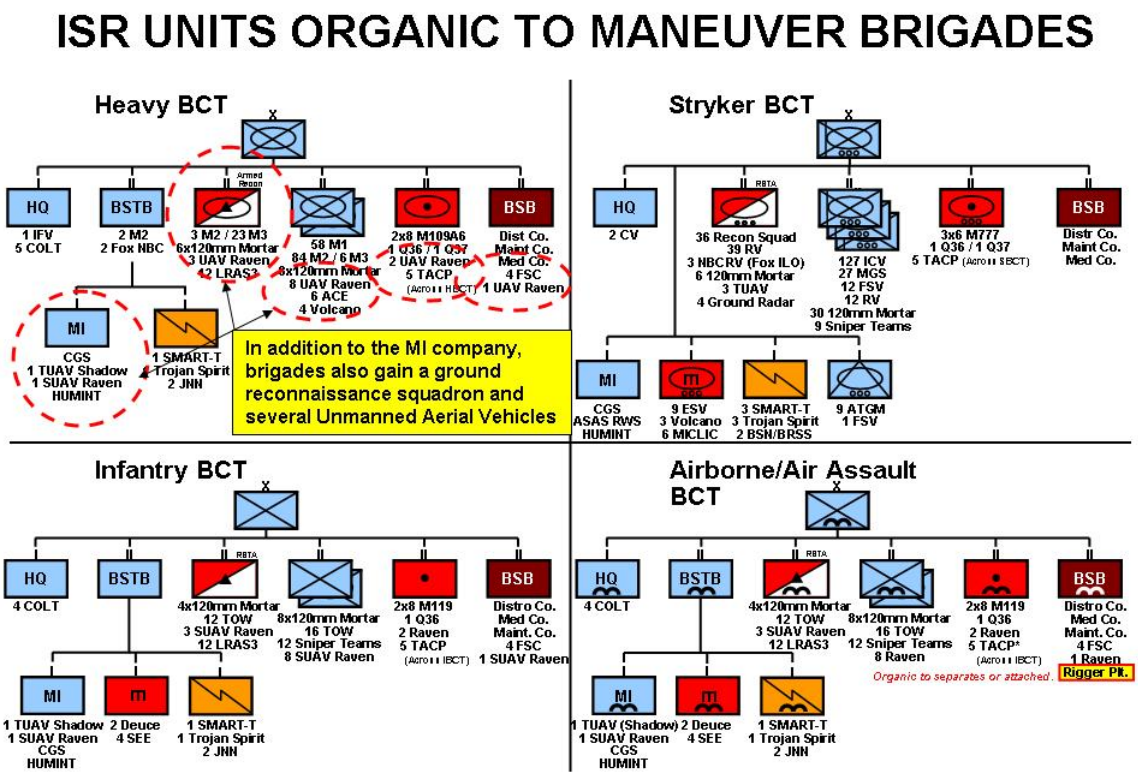

Figure 5: ISR assets of the modular brigade.

The modular brigade has organic ISR assets in multiple units. Derived from Director of Concept Development Briefing, *Current Force and Future Force: Military Intelligence Overview* (FT Huachuca: USAIC&FH, 23 June 2004).

The Army G2 is developing initiatives such as Project Foundry to help resolve some of these issues. Project Foundry is an initiative to strengthen Army intelligence skills for soldiers assigned to modular divisions and BCTs. Under this initiative, the Army would station a percentage of intelligence soldiers assigned to tactical units at intelligence organizations that are engaged in steady state, intelligence missions focused on target sets specific to that theater. Soldiers would train with their parent tactical unit at collective training events, but condition their

individual skills through experience and exposure to seasoned intelligence professionals. Project Foundry's goal is to provide technically proficient, regionally experienced and culturally knowledgeable intelligence personnel to round out the tactical modular intelligence forces.[113]

Another concern again facing the Army intelligence system's tactical echelon is human resources. The cost to resource the forward military intelligence capability is greater then the personnel on-account because the number of maneuver brigades is increasing as the Army transforms. This is causing a near term personnel shortage in the tactical military intelligence ranks. According to a May 2005 Congressional Research Service Report, "The Army has reportedly stated that it will require an additional 2,800 military intelligence specialists by the end of FY2005 to meet near-term shortages and an additional 6,200 by 2010 to meet modularity requirements."[114] Although fully staffing the tactical units is not a new challenge for Army intelligence, managing the problem at the division level will be more difficult. Without the CEWI battalion, there is no longer an administrative body to reallocate scarce resources on a mission-requirements basis.

[113] *Army Intelligence Comprehensive Guide to Modularity.* White paper prepared under the direction of the Army G2, sets forth the evolving plan for modular Future Force ISR, and provides a stepping off point for the planning and coordination required to implement the capabilities-based force. 11 May 2005, 17.

[114] Andrew Feickert, "US Army's Modular Redesign: Issues for Congress," *CRS Report for Congress*, (Washington, DC: Congressional Research Service, Library of Congress, 20 May 2005), 11.

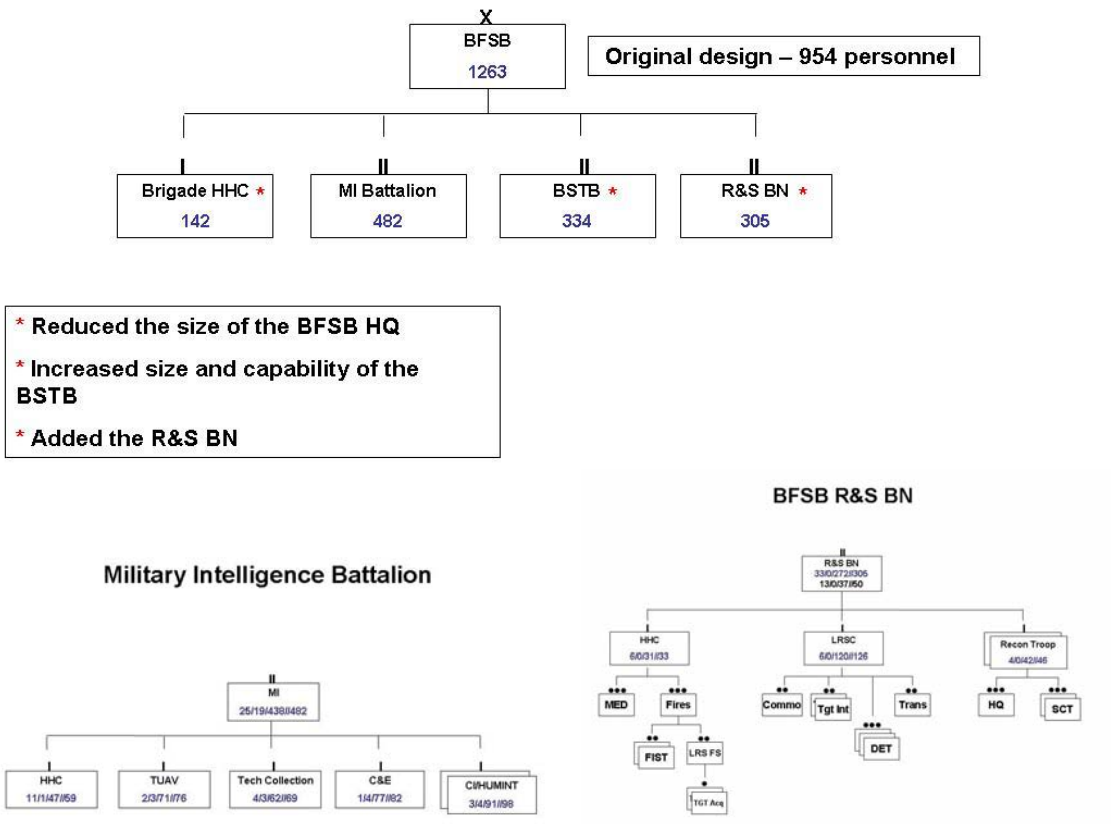

Figure 6. The organizational structure of the BFSB.

This BFSB redesign increases the ground reconnaissance capability significantly. From a briefing by Combined Arms Doctrine Directorate, *BFSB Design* (Fort Leavenworth, K.S.: November 2005).

The second change in modularity is the creation of a military intelligence battalion in support of the modular division, but not necessarily organic to it. Force designers originally called this unit the Reconnaissance, Surveillance, and Target Acquisition (RSTA) brigade and later renamed it the Battlefield Surveillance Brigade (BFSB). The BFSB is another capability that is suffering from the decision to place increased collection and analysis capabilities forward with the BCT. Many argue that the modular division still needs its own organic reconnaissance

and surveillance capability. This capability compliments and reinforces the ISR activities of its maneuver brigades and provides coverage over areas within the division area of operations that theater assets will not cover and brigade assets cannot cover. "The requirement for the [Military Intelligence] battalion within the [Reconnaissance and Surveillance] brigade is clear to meeting our HUMINT collection requirements in Iraq and Afghanistan," stated LTC Stephen K. Iwicki, Deputy Director of Task Force Actionable Intelligence in a report issued in the autumn of 2004.[115] The near term inability of the Army to resource these battalions may leave the division commander without general support intelligence assets critical to conducting simultaneous, noncontiguous operations against an irregular threat.

Intelligence capability gaps

The intelligence capability of a modular division cannot provide a focused and detailed understanding of a networked, irregular threat because it lacks the capability to provide regional social, religious, cultural, political, and military expertise. The results of this study support this conclusion with three observations. First, the modern, irregular threat may have chosen its organizational structure and asymmetric tactics for proactive, not reactive reasons; therefore, a central premise of the Army's theoretical threat model may be invalid. Second, the capabilities-based approach to force design may be insufficient for developing an intelligence organization.

[115] Stephen K. Iwicki, "CSA's Focus Area 16: Actionable Intelligence…one year later," *Military Intelligence Professional Bulletin* (October-December 2004), Accessed online from http://www.findarticles.com/p/articles/mi_m0IBS/is_4_30/ai_n13822278/print. LTC Iwicki was the Deputy Director of Task Force Actionable Intelligence (TF-AI) assigned to the Army G2. The article underscores the need for a division level intelligence collection capability. LTC Iwicki stated in full, "Another critical supporting element of the UEx is the MI battalion in the reconnaissance, surveillance, and target acquisition (RSTA) brigade. The RSTA brigade provides additional collection capabilities that represent the GS collectors for the UEx commander and a force pool of collectors to reinforce and augment BCT collection capabilities. While the RSTA brigades are a key element of the Modular Force, the Army is still determining the required number of these brigades; thus, none have activated to date. The requirement for the MI battalion within the RSTA brigade is clear and critical to meeting our HUMINT collection requirements in Iraq and Afghanistan. We envision there will eventually be ten MI battalions at the UEx echelon, independent of whether there is a RSTA brigade. We are activating the first MI battalion (UEx) at Fort Hood, Texas, in July 2005. We are working a strategy to have ten MI battalions (UEx) by the end of FY07. This is a significant challenge, but a capability our Army needs now."

Intelligence operations must provide specific information about a specific threat in order to be complete. The capabilities-based approach dissuades force designers from developing region-specific specialties. Third, the Army must consider a mix of functional, multi-divisional, and matrix, organizational structures to provide skill sets to subordinate division and brigade commanders tailored to their particular tactical problem. The sufficiency of the Army model, the underpinning concept of a capabilities-based approach, and a centering on modernization and reform in lieu of transformation contribute to the current set of intelligence capabilities shortfalls.

Is the Army's approach sufficient?

The key challenge for the United States is that it must balance the flexibility of generalization against the precision of specialization in order to have one intelligence system capable of understanding multiple threats. The capabilities-based model does not appear to provide this balance. In fact, it may be counterintuitive when applied to intelligence operations and analysis. The purpose of intelligence is to provide specific information and analysis about the threat that the commander must know in order to make decisions and accomplish his mission. FM 2-0, *Intelligence* states, "The commander must understand how current and potential enemies organize, equip, train, employ, and control their forces. *Intelligence provides an understanding of the enemy,* which assists in planning, preparing, and executing military operations."[116] (Emphasis added). Intelligence is inherently threat centered.

Some have stated that U.S. dominance in conventional warfare has forced the emerging threat to choose a networked organizational structure and asymmetric tactics. It assumes the threat would prefer to form a conventional army and conduct conventional warfare, but it cannot afford to solely because of the associated tactical risks. The characteristics of the strategic environment support a competing hypothesis. The modern, irregular threat may prefer the

[116] Headquarters, Department of the Army, *FM 2-0: Intelligence.* (Washington D.C: 17 May 2004), 1-1.

networked organizational structure and set of asymmetric tactics for proactive, not reactive, reasons such as the economies of scale it provides and the tactical advantage it provides through the denial of U.S. technological advantages. By using the global information grid and transportation network that the U.S. relies on for its own economy, the threat exploits an existing infrastructure to satisfy its logistical and operational needs without the need to invest in its own costly infrastructure. The threat also exploits the advantages of a networked organization embedded in a civilian population to deny the United States its technological advantages. The Soviet threat model presented conventional signatures that the existing intelligence system is designed to collect and analyze. The existing specialties and technologies are not capable of identifying and understanding the indications and warnings presented by a networked organization.

To understand and exploit networked organizations, Army intelligence must arm its divisions and brigades with analysts that are proficient in advanced social network analysis techniques. Social network analysis "explores the structures of groups in human society by modeling individuals, places, and objects as nodes of a graph, and adding links between nodes to represent relations among them."[117] The Army trains analysts in elementary link analysis techniques, a form of social network analysis, but does not train the soldiers to the level of sophistication needed to exploit elaborate networks.

Network Text Analysis is one example of the skills modern analysts need to be effective at mapping networks such as Al Qaeda. Network Text Analysis is a method of encoding words in texts and constructing network diagrams from that data. Jana Diesner and Kathleen Carley of Carnegie Mellon University provide a good overview of the method in their paper "Using Network Text Analysis to Detect the Organizational Structure of Covert Networks." In their

[117] D.B. Skillicorn, "Social Network Analysis via Matrix Decompositions: al Qaeda," School of Computing (Queens University, Kingston, Ontario: 2004), 1. Accessed online from http://www.cs.queensu.ca/~skill/alqaeda.pdf.

work, they use map analysis of words in text to create a network model displaying the links between the words with the goal of revealing social structures from the texts.[118] Such techniques in a division could significantly improve the value of document exploitation and its fusion with information gained from other intelligence disciplines.

Still, it is clear that no single organization can provide complete intelligence support to the modular division in the contemporary operational environment. It is equally clear that no single organizational structure will optimize the intelligence capability of the Army. The organizational structures of the systems within the Army intelligence system must demonstrate the strengths most often required for its primary purpose. The modular division's tactical reconnaissance and surveillance capabilities must be highly adaptable to multiple environments to support the division's global design. This demands that the division's capabilities be general in nature. A multi-divisional organization that provides dedicated generalists to the maneuver commander is most likely more useful than dedicated regional experts that may or may not deploy to their aligned region. The modular division's intelligence capability must also be interoperable with all theater and national capabilities in order to provide input into and receive products from the national intelligence enterprise. In this manner, the modular division's ability to integrate a matrix organization consisting of specialists from across the national intelligence enterprise is vital to its ability to provide the knowledge necessary to be predictive. The most significant organizational innovation that developed because of recent operations in the GWOT is the Joint Inter-Agency Task Force (JIATF). The JIATF concept is a matrix organization that assembles interagency specialists centered on achieving a specific task. Rear Admiral (Retired)

[118] Jana Diesner and Kathleen M. Carley, "Using Network Text Analysis to Detect the Organizational Structure of Covert Networks," Center for Computational Analysis of Social and Organizational Systems (CASOS), Institute for Software Research International (ISRI), School of Computer Science, Carnegie Mellon University, Accessed online from author's website at http://www.andrew.cmu.edu/user/jdiesner/publications/NAACSOS_2004_Diesner_Carley_Detect_Covert_Networks.pdf.

Ralph D. Utley commented before the 109th Congress that, "The Joint Interagency Task Force model works. In particular, Joint Interagency Task Force South (JIATF-S) in Key West has become a powerful interagency and international team that is fusing information from law enforcement agencies, the Intelligence Community and our international partners. This combined interagency and international task force is producing remarkable results and has improved the effectiveness of our detection, monitoring and end-game platforms."[119] The success of JIATFs suggests that commanders must tailor the specialties required to counter the threat to their specific tactical problem.

Theater capabilities, such as the Theater Intelligence Brigade, must remain regionally focused to provide the expert level of knowledge about the nuances of that specific region. At this level, functional organizations delineated by intelligence discipline that conduct operations in support of the theater commander will continue to make sense. Coupled with the modular division's ability to receive specialty teams, this capability provides the overwatch necessary to ensure the maneuver commander receives continuous support throughout his operation.

A mix of functional, multi-divisional, and matrix organizations can provide the flexibility the Army needs to tailor its divisional intelligence capability to the characteristics of specific threats. Given the short-term limitations to technological solutions and the requirement for a wide variety of joint and interagency skills, innovative use of organizational structures within the theater Army can increase the division commander's ability to maximize limited resources and tailor his intelligence system to the specific threat he faces. Training in modern analytical techniques such as social network analysis is critical to maximizing these limited resources. Intelligence assets will continue to be finite as the adversaries of the new multi-polar world grow. Leadership must provide the discipline to allocate the right resource the right problem at the right

[119] House Committee on International Relations, *Statement Of RADM Ralph D. Utley, USCG (Ret.), Acting United States Interdiction Coordinator, on Plan Colombia: Major Successes and New Challenges*, 109th Congress, May 11, 2005. 1.

time. Leaders' greatest challenge will remain constraining the desire to re-task regional specialists as generalists in reaction to an unforeseen crisis. Mismanagement of the Army's intelligence soldiers will result in a diffusion of expertise and a loss of understanding of the threat in its many regional manifestations.

APPENDIX A. Primer on Organizational Structure

The purpose of this appendix is to familiarize the reader with the various forms of organizational structure presented in *Organization Theory* by Mary Jo Hatch. It consists of six structures relatively organized from least to most complex. The reader should refer back to figure 1 for examples of each organizational structure.

The first organizational structure category is the Simple Structure. It is a set of completely flexible relationships. It has low levels of complexity resulting from limited differentiation. Normally, it is the first type of organizational structure to develop anytime two or more individuals come together in a common undertaking. Interpersonal relationships established within a small working group are an example of a Simple Structure.[120]

The second organizational structure is the Functional Structure. It groups activities according to logic of similarity in work functions produced by interdependent tasks and common goals and it maximizes economies of scale from specialization.[121] It is efficient in the sense that there is limited duplication of effort. The Army of Excellence divisional military intelligence battalion when in garrison and several strategic military intelligence battalions have functional structures. By pooling like MOSs into functional companies, the unit could gain efficiencies in training time and resources. Similarly, strategic units organized along functional lines gain efficiencies in their operational mission by pooling resources for administration and deploying them in tailored packages to meet the requirements of the mission.

The third organizational structure is Multi-divisional Structure, or M-structure. Organizations usually employ it as a means to alleviate overburdened centralized decision makers. It consists of a set of separate functional structures that reports to a headquarters staff. Brigade Combat Teams are an example of multi-divisional structures. Although the intent behind

[120] Hatch, *Organization Theory*, 183.
[121] Ibid., 183.

the design is to alleviate overburdened decision makers, it can create the need for more overhead. Hatch notes, "When multi-divisional form is created out of a functional structure, the first move is to construct several small functional organizations from the larger one. Each of the smaller organizations operates as a separate functional organization with one main difference, because of the interdependence between the divisions, a higher level of coordination is required that is not needed by the purely functional structure. [It] is provided by the headquarters staff and executive level of the hierarchy."[122]

The fourth organizational structure is the Matrix Structure. This design combines the efficiency of the functional structure with the flexibility and responsiveness of the division structure. It is the result of super-imposing two structures superimposed on each other. It consists of a functional structure and a project structure. The functional structure allocates specialists to projects and is responsible for the training and administration of the specialists. The project structure oversees project execution and manages project resources.[123]

The greatest benefit of a matrix organization is flexibility. When the organization's leadership identifies a new project, they only need to identify a project leader and allocate the appropriate specialists to him or her. Functional and divisional organizations require major structural adjustments before they can adapt to a new project. A matrix organization also benefits by maximizing the value of its specialists. A matrix organization maximizes the utilization period of its specialists by pooling them and allocating them to projects only when the project needs the specialists' talents. They can prioritize the specialists among the projects based on the project leaders' needs. Multi-divisional organizations retain specialists in each division on a permanent basis. This may lead to large periods of underutilization of the specialists depending on the nature and phase of their current project. Functional organizations also underutilize

[122] Ibid., 184-185.
[123] Ibid., 187-188.

specialists by retaining them in their pools despite the project load or balance. An organization that is functionally aligned may experience significant "down time" by function as they execute their operational cycle.[124]

The fifth organizational structure is a hybrid structure that combines aspects of matrix, divisional, and functional organizational structures. They may result from decisions by the organization's leadership or they may emerge out of a changing organization.[125] Hybrid structures are common when an organization contains multiple echelons. Within the Army intelligence system, various echelons employ different organizational structures, but when observed as an interoperable whole, the system is classified as a hybrid structure.

The final organizational structure is a network structure. In a network organization, lateral relationships replace most vertical communication and control relationships. According to Hatch, they seem most likely to form when organizations face rapid technological change, shortened product lifecycles, and fragmented, specialized markets. They can also be the result of massive outsourcing. Network organizations have their own mix of advantages and disadvantages. They encourage information sharing, liberate decision-making, inspire innovation, and enable rapid information exchange through their lateral relationships. However, they must rely on working together voluntarily which demands a high level of teamwork. Network partners may also undermine network effectiveness by pursuing self-interest. Therefore, the leadership of a network organization must work at developing and maintaining an organizational identity and sense of purpose and overcome both geographic diversity and loosely coupled interests and activities.[126]

[124] Ibid., 190.
[125] Ibid., 190.
[126] Ibid., 191.

APPENDIX B. Complex Adaptive Systems Terminology.

This appendix provides the reader with definitions and explanations of terms used to describe complex adaptive systems. Complex adaptive systems consist of agents, strategies, artifacts, and populations. They interact with their environment and select changes that result in improvements to the system. They adapt in order to survive.

Agents, strategies, artifacts, and populations are the components of a system. Axelrod defines an agent as an entity that can interact with its environment and other agents purposefully. Although people are the most common concept of an agent, an agent can also be an organization such as a team or a thing such as a computer system that is capable of interacting with its environment. Strategies are "the way an agent responds to its surroundings and pursues its goals."[127] They can be both deliberate, such as the Department of Defense *Transformation Planning Guidance*, or they can emerge from the pursuit of a goal. Agents can measure their strategies against a standard or measure of success. Strategies can change over time because of changes in agents and populations.

Artifacts are the entities agents use. They usually do not have a purpose on their own, but agents use them to interact with the system. A collection platform is an example of an artifact. It derives its value from its capability and its location within the system and its use by an agent.

Populations are groupings of agents and sometimes strategies. They have structure and at least one common trait. These elements combined create a system. Axelrod defines a system as "one or more populations of agents, all the strategies of the agents, along with the relevant artifacts and environmental factors."[128] He defines a system as complex “when there are strong

[127] Axelrod and Cohen, 4.
[128] Ibid., 6.

interactions among its elements, so that current events heavily influence the probabilities of many kinds of later events."[129]

One way that a complex system can change is through the selection of a different strategy. Selection of a different strategy can be deliberate or emergent. Agents can learn from their environment and peers to identify strategy changes, they can select new strategies by trial and error, and they can select new strategies as the result of changes to their populations. Selection may or may not lead to improvements in the system. Axelrod refers to the instances of selection that result in a measurable improvement as adaptation. He combines these concepts to describe a Complex Adaptive System as, "a system (that) contains agents or populations that *seek* to adapt."[130]

[129] Ibid., 7.
[130] Ibid., 7. Emphasis in original.

APPENDIX C. Acknowledgements.

The following individuals provided great insight and were instrumental in developing this monograph.

LTG David Petraeus, COL Kenneth Devan, COL George Franz, COL Hugh Smith, COL Mark Solseth, LTC Andrew Fowler, MAJ Bruce Murphy, Mr. Michael Brake, Mr. Steven Jones, Mr. John Sanders, Mrs. Kellie Smith, Mr. Rex Williams, and my SAMS classmates.

BIBLIOGRAPHY

Books

Axelrod, Robert and Michael D. Cohen. *Harnessing Complexity*. New York: Basic Books, 2000.

Gunaratna, Rohan. *Inside Al Qaeda*. New York: Columbia University Press, 2002; Berkley Books, 2003.

Hatch, Mary Jo. *Organization Theory.* New York: Oxford University Press, 1997.

Huntington, Samuel. *The Clash of Civilizations.* New York: Touchstone Books (Simon & Schuster, Inc.), 1997.

Knox, MacGregor and Williamson Murray, eds, *The Dynamics of Military Revolution, 1300-2050.* Cambridge: Cambridge University Press, 2001. Reprint, New York: Cambridge University Press, 2003.

Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: W. W. Norton, 2001.

Murray, Williamson and Allan R. Millett, eds. *Military Innovation in the Interwar Period.* Cambridge: Cambridge University Press, 1996; Cambridge, 1998.

O'Neill, Bard E., *Insurgency & Terrorism: From Revolution to Apocalypse.* Washington, DC: Potomac Books, Incorporated, 2005.

Sageman, Marc. *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2004.

Warner, Michael. "Intelligence Transformation: Past and Future." In *Rethinking the Principles of War*, ed. Anthony D. McIvor, 516-532. Annapolis: Naval Institute Press, 2005.

U.S. Government Publications

Army Intelligence Comprehensive Guide to Modularity. White paper prepared under the direction of the Army G2, sets forth the evolving plan for modular Future Force ISR, and provides a stepping off point for the planning and coordination required to implement the capabilities-based force. 11 May 2005.

Department of State, Office of the Coordinator for Counterterrorism. *Country Reports on Terrorism 2004.* Washington, DC: Department of State Multimedia Services, April 2005. Department of State Publication 11248.

Headquarters, Department of the Army. *United States Army 2004 Army Transformation Roadmap*. Washington, D.C.: Army Transformation Office, July 2004

Headquarters, Department of the Army. *FM 1-02: Operational Terms and Graphics*. Washington, D.C.: GPO, September 2004.

Headquarters, Department of the Army. *FM 2-0: Intelligence.* Washington, D.C.: GPO, 17 May 2004.

Headquarters, Department of the Army. FM 3-0, *Operations.* Washington, D.C.: GPO, June 2001.

Headquarters, Department of Defense, *JP 1-02: DOD Dictionary of Military and Associated Terms.* Washington, D.C.: GPO, 12 April 2001, as amended through 31 August 2005.

Headquarters, Department of Defense. *National Defense Strategy of the United States of America*. Washington, D.C.: GPO, 2005.

Headquarter, Department of the Army. *Army Strategic Planning Guidance, Appendix D: The Security Environment*, Washington D.C.: GPO, 2005, accessed online at http://www.army.mil/references/ASPG-AnnexD.doc.

Headquarters, Department of Defense. *National Military Strategy of the United States of America*. Washington, DC: GPO, 2004.

Headquarters, Department of Defense. *Quadrennial Defense Review Report.* Washington D.C.: GPO, 2001.

Headquarters, Department of Defense, *Transformation Planning Guidance.* Washington, D.C.: GPO, April 2003.

Headquarters, Joint Forces Command. *The Joint Operational Environment: Into the Future.* Coordinating Draft, January 2005.

NSC 68: United States Objectives and Programs for National Security (April 14, 1950), Section VI: U.S. Intentions and Capabilities—Actual and Potential, A: Political and Psychological. Accessed online at http://www.mtholyoke.edu/acad/intrel/nsc-68/nsc68-1.htm.

Office of the President of the United States. *The National Security Strategy of the United States of America.* Washington DC, September 2002.

U.S. Congress. House. Committee on International Relations. *Statement Of RADM Ralph D. Utley, USCG (Ret.), Acting United States Interdiction Coordinator, on Plan Colombia: Major Successes and New Challenges*. 109th Congress. May 11, 2005.

Articles and Professional Journals

Barnett, Thomas P.M. “The Pentagon’s New Map,” *Esquire*, March 2003, accessed from Thomas Barnett’s website at http://www.thomaspmbarnett.com/published/pentagonsnewmap.htm.

Barnett, Thomas P.M. and Henry H. Gaffney, Jr. “The Global Transaction Strategy,” *Military Officer*, May 2003, accessed online at http://www.thomaspmbarnett.com/published/gts.htm.

Burlas, Joe. “Initiatives Seek to Transform Army Intelligence Capabilities.” *Army News Service* 13 April 2004, accessed online from http://www4.army.mil/ocpa/print.php?story_id_key=5848.

Finnegan, John and Romana Danysh. *Military Intelligence.* Washington, D.C.: United States Army Center of Military History, 1998.

Harris, Shane. “Army Project Illustrates Promise, Shortcomings of Data mining.” *National Journal*. Accessed online from Govexec.com homepage at http://www.govexec.com/dailyfed/1205/120705nj1.htm.

Iwicki, Stephen K. “CSA’s Focus Area 16: Actionable Intelligence: National, Joint, and Expeditionary Capabilities.” *Military Intelligence Professional Bulletin* (July-September 2004). Accessed online from http://www.findarticles.com/p/articles/mi_m0IBS/is_3_30/ai_n13821812/print.

_____. “CSA’s Focus Area 16: Actionable Intelligence…one year later.” *Military Intelligence Professional Bulletin* (October-December 2004). Accessed online from http://www.findarticles.com/p/articles/mi_m0IBS/is_4_30/ai_n13822278/print.

Morris, Michael F. "Al Qaeda as Insurgency." *Joint Forces Quarterly* #39. Washington, DC: Institute for National Strategic Studies, October 2005. Available online at http://www.dtic.mil/doctrine/jel/jfq_pubs/issue39.htm.

Stern, Jessica. “The Protean Enemy (al Queda (sic)).” In *Foreign Affairs*, 01 July 2003. Accessed online from http://www.ksg.harvard.edu/news/opeds/2003/stern_protean_enemy_foraffairs_070103.htm

Miscellaneous

Arquilla, John, David Ronfeldt, and Michele Zanini. “Networks, Netwar, and Information-Age Terrorism,” in Ian O. Lesser et al., *Countering the New Terrorism*. Santa Monica.: The RAND Corporation, MR-989-AF, 1999.

Chambers, Jay, Michael Morgan, Lou Antonetti, Charles Carson, Peter Curry, Leslie Curtin, Keith Miller, John Munoz-Atkinson, Richard Shrank, Mark Tapper, Richard Williams, eds. *Combating Terrorism in a Globalized World: Report by the National War College Student Task Force on Combating Terrorism.* Washington, DC: National Defense University, November 2002, accessed online at http://www.au.af.mil/au/awc/awcgate/ndu/n02combating_terrorism.pdf.

Diesner, Jana and Kathleen M. Carley. “Using Network Text Analysis to Detect the Organizational Structure of Covert Networks.” Center for Computational Analysis of Social and Organizational Systems (CASOS), Institute for Software Research International (ISRI), School of Computer Science, Carnegie Mellon University. Accessed online from author’s website at http://www.andrew.cmu.edu/user/jdiesner/publications/NAACSOS_2004_Diesner_Carley_Detect_Covert_Networks.pdf.

Feickert, Andrew. “US Army’s Modular Redesign: Issues for Congress.” *CRS Report for Congress*. Washington, DC: Congressional Research Service, Library of Congress, 20 May 2005.

Garfinkel, Simson L. “Leaderless Resistance Today.” Accessed online from http://www.firstmonday.org/issues/issue8_3/garfinkel.

“Globalization: Threat or Opportunity?” International Monetary Fund Website, April 12, 2000 (Corrected January 2002), accessed from http://www.imf.org/external/np/exr/ib/2000/041200.htm.

Sandoz John F. *Red Teaming: Shaping the Transformation Process* Alexandria: Institute for Defense Analysis, 2001. IDA, D-2590.

Skillicorn, D.B. “Social Network Analysis via Matrix Decompositions: al Qaeda.” School of Computing website (Queens University, Kingston, Ontario: 2004). 1. Accessed online from http://www.cs.queensu.ca/~skill/alqaeda.pdf.